March 2026

Digital Omnibus

ACEA position and amendements

RECOMMENDATIONS

I. DATA ACQUIS

1. Reject the proposal to amend the definition of data holder in Article 1(2)(b) of the Proposal.
2. Amend the definition of “machine-readable data” to encompasses data transmitted through any on-device or remote-server communication interface in Article 1(2)(e) of the Proposal.
3. Delete the reference to “data users” in the definition of “permission” in article 2(4)(b) of the Proposal.
4. Extend the financial penalty regime set out in Article 40 of the Data Act to data intermediation service providers and data altruism organisations in Article 1(18) of the Proposal.
5. Expand the proposed membership of the European Data Innovation Board to include industry and service representatives in Article 1(22) of the Proposal.
6. Consolidate Articles 4(13) and (14) of the Data Act into a single, comprehensive provision governing the use of readily available data that is non-personal.
7. Repeal *ex ante* notification requirements laid down in the Data Act to ease administrative burden for data holders and notified bodies (Articles 4(2), (7), (8); 5(10), (11); 8(3)).
8. Repeal requirements of the Data Act for data holders to disclose information setting out the basis for the calculation of the compensation to third parties (Articles 9(7) and 20(2)).
9. Repeal Article 32 of the Data Act on the transfer of data to third countries; relevant GDPR provisions should exclusively apply to international data transfers.
10. Repeal Article 20a(3) of the Renewable Energy Directive (EU) 2023/2413.

II. DATA PROTECTION AND PRIVACY

1. Permit further processing of data for scientific research purposes supporting innovation, even when conducted by private companies for commercial purposes.
2. Amend rules on the processing of special categories of personal data for AI by narrowing the prohibition to processing which directly reveals sensitive attributes about a data subject, revising the restrictions in Article 9(5) to enable meaningful use and sharing of processed data, and broadening the new exception under Article 9(2)(k) in a technology-neutral manner.
3. Limit the documentation requirements in Article 33(5) GDRP to breaches that are likely to result in a high risk to the rights and freedoms of natural persons.

4. Expand the Commission's empowerment under the proposed new Article 41a to other areas including codes of conduct and certification.
5. Amend the proposed new rules for access and storage to the data held on a users' devices by allowing the storage of and access to data on terminal equipment based on any lawful processing ground of the GDPR, amending the new Article 88a(3)(b) to refer to the "data subject or subscriber", and ensuring full alignment of EU rules on the processing of both personal and non-personal data.
6. Incorporate the EU principle of proportionality, as enshrined in Article 5(4) TEU, into Article 5 GDPR.

III. CYBERSECURITY

1. Standardise the process for reporting relevant incidents under all relevant EU cybersecurity instruments, developing standard templates and defining a set of criteria for reporting, common to all member states.
2. Adopt a risk-based approach to cybersecurity reporting by exempting small-entities, limiting requirements to information systems that support critical and highly critical activities, and establishing a single, harmonised set of security measures at EU level based state-of-the-art standards.

PROPOSED AMENDMENTS TO THE DIGITAL OMNIBUS

I. DATA ACQUIS

1. Revision of the definition of 'data holder'

Proposal for amendment

Proposal for a regulation **Article 1, para. (2)**	
Text proposed by the Commission	*Amendment*
(b) point (13) is replaced by the following: ***'(13) 'data holder' means a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use or make available data, including, where contractually agreed, product data or related service data, which it has retrieved or generated during the provision of a related service;***	***Deleted***
Justification: The cumulative requirement to "use" and to "make available data" in the definition of data holders ensures that obligations under the Data Act attach only to actors that exercise meaningful control over data and can comply with these obligations. Changing this would extend the requirements of the Data Act to entities that merely have a limited or technical right to use data or that are under a narrow obligation to pass it on without exercising any real control over it and thus lack the legal authority or practical ability to make data available, such as data intermediation service providers. This expansion creates legal uncertainty for businesses, jeopardises the neutrality of data intermediation service providers, and risks imposing obligations on entities that are structurally unable to comply with the Data Act's requirements, potentially placing them in conflict with contractual or legal restrictions.	

2. Addition of the Definition of 'machine-readable data'

Proposal for amendment

Proposal for a regulation **Article 1, para. (2), point (e)**	
Text proposed by the Commission	*Amendment*
(58) 'machine readable format' means a ***file*** format structured so that software applications can easily identify, recognise and extract specific data,	(58) 'machine-readable format**"** means a format **or** ***representation of data*****,** structured so that software applications can easily identify, recognise and extract

including individual statements of facts, and their internal structure;	specific data, including individual statements of facts and their internal structure***, irrespective of the medium through which it is made available.***
Justification: This definition originates from a context focused on documents and file formats which does not reflect the operational environment to which the Data Act applies, where the primary focus is on the exchange of product data and related service data through machine-to-machine communication interfaces, rather than files. This misalignment becomes evident in practical settings such as connected vehicles, where data is accessed through continuous streams on in-vehicle interfaces like the CAN bus via the OBD connector, and not through files of any kind.	

3. Addition of the Definition of 'Permission'

Proposal for amendment

Proposal for a regulation **Article 1, para. (2), point (a)**	
Text proposed by the Commission	*Amendment*
(4b) 'permission' means giving ***data users*** the right to the processing of non-personal data;	(4b) 'permission' means giving the right to the use of non-personal data;
Justification: This definition from the Data Governance Act relies on the concept of 'data user', which was not included in the proposal and conflicts with the Data Act's concept of 'user', creating uncertainty as to its interpretation. To ensure legal certainty, the reference to "data users" should be deleted.	

4. Harmonising Penalties for non-compliance

Proposal for amendment

Proposal for a regulation **Article 1, para. (18)**	
Text proposed by the Commission	*Amendment*
Article 32g *Monitoring of compliance* (1) The competent authorities referred to in Article 32b shall, either on their own initiative or on a request by a natural or legal person, monitor and supervise whether recognised data intermediation services providers and recognised data altruism organisations comply with the requirements laid down in this Chapter, including whether they continue to comply with the requirements for registration laid down therein. (2) The competent authorities shall have the power to request from recognised data intermediation	Article 32g *Monitoring of compliance* (1) The competent authorities referred to in Article 32b shall, either on their own initiative or on a request by a natural or legal person, monitor and supervise whether recognised data intermediation services providers and recognised data altruism organisations comply with the requirements laid down in this Chapter, including whether they continue to comply with the requirements for registration laid down therein. (2) The competent authorities shall have the power to request from recognised data intermediation

services providers or recognised data altruism organisations, or their legal representative, all the information that is necessary to verify compliance with the requirements laid down in this Chapter. Any request for information shall be proportionate to the performance of the task and shall be reasoned. (3) Where a competent authority finds that a recognised data intermediation services provider or a recognised data altruism organisation does not comply with one or more of the requirements laid down in this Chapter, it shall notify that entity, or its legal representative, of those findings and give it the opportunity to state its views, within 30 days of the receipt of the notification. (4) The competent authority shall have the power to require the cessation of the non-compliance referred to in paragraph 3 either immediately or within a reasonable time limit and shall take appropriate and proportionate measures with the aim of ensuring compliance. (5) If a recognised data intermediation services provider or a recognised data altruism organisation does not comply with one or more of the requirements laid down in this Chapter even after having been notified in accordance with paragraph 3, that entity shall: (a) lose its right to use the label referred to in Article 32a in written and spoken communication; (b) be removed from the public Union register referred to in Article 32a. Any decision revoking the right to use the label as referred to in the first subparagraph, point (a), shall be made public by the competent authority.	services providers or recognised data altruism organisations, or their legal representative, all the information that is necessary to verify compliance with the requirements laid down in this Chapter. Any request for information shall be proportionate to the performance of the task and shall be reasoned. (3) Where a competent authority finds that a recognised data intermediation services provider or a recognised data altruism organisation does not comply with one or more of the requirements laid down in this Chapter, it shall notify that entity, or its legal representative, of those findings and give it the opportunity to state its views, within 30 days of the receipt of the notification. (4) The competent authority shall have the power to require the cessation of the non-compliance referred to in paragraph 3 either immediately or within a reasonable time limit and shall take appropriate and proportionate measures with the aim of ensuring compliance. (5) If a recognised data intermediation services provider or a recognised data altruism organisation does not comply with one or more of the requirements laid down in this Chapter even after having been notified in accordance with paragraph 3, that entity shall: (a) lose its right to use the label referred to in Article 32a in written and spoken communication; (b) be removed from the public Union register referred to in Article 32a. ***(c) be subject to the penalties referred to in Article 40;*** Any decision revoking the right to use the label as referred to in the first subparagraph, point (a), shall be made public by the competent authority ***(6) Notwithstanding any administrative or non-judicial remedy, any affected natural or legal person shall have the right to effective judicial remedy pursuant to Article 39.***
Justification: Article 32(g) introduces sanctions for breaches of data intermediation rules which diverge markedly from those applicable under the Data Act itself in Article 40. Data intermediation service providers and data altruism organisations are only subject to non-financial corrective measures, while other actors face financial penalties for comparable infringements.	

This results in unequal treatment of similar non-compliance, undermining both effectiveness and fairness. Non-financial measures offer limited deterrence, fail to address the economic harm suffered by data holders, and distort the regulatory balance by shielding intermediaries from financial liability while exposing data holders to significant fines.

The financial penalty regime set out in Article 40 of the Data Act should be extended to data intermediation service providers and data altruism organisations to ensure equal treatment, restore competitive neutrality, and provide a credible deterrent against non-compliance across the entire data-sharing ecosystem.

5. Bringing balance to the European Data Innovation Board

Proposal for amendment

Proposal for a regulation **Article 1, para. (22)**	
Text proposed by the Commission	*Amendment*
'Article 41a European Data Innovation Board (1) The European Data Innovation Board is established as a means to advising and assisting the Commission in coordinating the enforcement of this Regulation and to serve as a forum of discussion for the development of a European data economy and data policies. (2) It shall be composed at least of representatives of Member States competent for matters related to data, the competent authorities for enforcement of Chapters II, III, V, VIIa and VIIc of this Regulation, the European Data Protection Board, the European Data Protection Supervisor, ENISA, the EU SME Envoy or a representative appointed by the network of SME envoys. The Commission may decide to add additional categories of members. In its appointments of individual experts, the Commission shall aim to achieve gender and geographical balance among the members of the group. (3) The Commission shall decide on the composition of the different configurations in which the Board will fulfil its tasks. (4) The Commission shall chair the meetings of the European Data Innovation Board.'	'Article 41a European Data Innovation Board (1) The European Data Innovation Board is established as a means to advising and assisting the Commission in coordinating the enforcement of this Regulation and to serve as a forum of discussion for the development of a European data economy and data policies. (2) It shall be composed at least of representatives of Member States competent for matters related to data, the competent authorities for enforcement of Chapters II, III, V, VIIa and VIIc of this Regulation, the European Data Protection Board, the European Data Protection Supervisor, ENISA, ***EU Industry and Services representatives,*** the EU SME Envoy or a representative appointed by the network of SME envoys. The Commission may decide to add additional categories of members. In its appointments of individual experts, the Commission shall aim to achieve gender and geographical balance among the members of the group. (3) The Commission shall decide on the composition of the different configurations in which the Board will fulfil its tasks. (4) The Commission shall chair the meetings of the European Data Innovation Board.'
Justification: The proposed structure of the European Data Innovation Board (EDIB) under Article 41(a)(2) is unbalanced as it excludes key private stakeholders, and especially data holders who are essential to the implementation of data strategies. Membership of the EDIP should be extended to industry and service representatives to ensure fair coordination across all economic sectors and provide a holistic understanding of the European data economy by giving a voice to the private companies that are responsible for data deployment.	

6. Legal basis for non-personal data processing under the Data Act

Proposal for amendment

Proposal for a regulation **Article 1, paragraph 3a NEW**	
Text proposed by the Commission	*Amendment*
New	***3a. Article 4, paragraph 13, is replaced by the following:*** ***(13) A data holder shall only use any readily available data that is non-personal data if and to the extent that at least one of the following applies:*** ***(a) the user has given permission to the use of the non-personal data for one or more specific or general purposes;*** ***(b) its use is necessary for the performance of a contract to which the user is party or from which the user benefits, or in order to take steps at the request of the user prior to entering into a contract;*** ***(c) its use is necessary for compliance with a legal obligation to which the data holder is subject;*** ***(d) its use is necessary for the purposes of the legitimate interests pursued by the data holder or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the user.*** ***A data holder shall not use the data to derive insights about the economic situation, assets and production methods of, or the use by, the user in any manner that could undermine the commercial position of that user on the markets in which the user is active.***
Justification: The Data Act relies exclusively on the contractual consent of the user for non-personal data processing. This restrictive approach needlessly limits the legitimate and beneficial use of such non-personal data, especially for research and development, product improvement, quality control, safety, security or AI-driven innovation. The Data Act lays down a more restrictive framework for the use of non-personal data than the GDPR does for the processing of personal data. This provides an incentive for data holders to rely more heavily on personal data, which are inherently more sensitive, yet less burdensome to process, than non-personal data.	

At the same time, this requirement generates legal uncertainty by creating internal inconsistencies. It is unclear whether anonymised data falls within Articles 4(13) and 4(14), which risks discouraging anonymisation, as the use of personal data is less restricted under the GDPR than it is under the Data Act once anonymised. Consolidating Articles 4, paragraphs 13 and 14 into a single, comprehensive provision to govern the use of readily available data that is non-personal, and exempt anonymised data, will reinforce data protection principles by ensuring that organisations prioritise non-personal data and do not revert to personal data as a workaround.

Proposal for amendment

Proposal for a regulation **Article 1, paragraph 3b NEW**	
Text proposed by the Commission	*Amendment*
New	**3b. Article 4, paragraph 14, is deleted.**
Justification: Consistency with previous amendment.	

7. Reporting obligations under the Data Act

Proposal for amendment

Proposal for a regulation **Article 1, para. (3)**	
Text proposed by the Commission	*Amendment*
3. **in** Article 4, ***paragraph 8 is replaced by the following***: '8. In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the user poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse on a case-by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of	3. Article 4 **is amended as follows:** **(a) Paragraph 2 is amended as follows:** **'2. Users and data holders may contractually restrict or prohibit accessing, using or further sharing data, if such processing could undermine security requirements of the connected product, as laid down by Union or national law, resulting in a serious adverse effect on the health, safety or security of natural persons. Sectoral authorities may provide users and data holders with technical expertise in that context.;** **(b) Paragraph 7 is amended as follows:** **'7. Where there is no agreement on the necessary measures referred to in paragraph 6, or if the user fails to implement the measures agreed pursuant to paragraph 6 or undermines the confidentiality of the trade secrets, the data holder may withhold or, as**

confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to the user without undue delay. ***Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37***.';	**the case may be, suspend the sharing of data identified as trade secrets. The decision of the data holder shall be duly substantiated and provided in writing to the user without undue delay.;** **(c) Paragraph 8 is replaced by the following:** '8. In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the user poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse on a case-by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to the user without undue delay.';
Justification: The Data Act provides significant *ex-ante* reporting obligations on data holders. These requirements force data holders to notify national competent authorities of their decisions pro-actively even where these do not give rise to a dispute These requirements create unnecessary administrative burden on data holders as they require generating and communicating extensive documentation, which is likely to overwhelm competent authorities, and is unnecessary as these authorities are empowered to request any information, they see fit from data holders to verify compliance with the Data Act. Repealing these requirements will ease the administrative burden they create for data holders and competent authorities.	

Proposal for a regulation **Article 1, para. (4)**	
Text proposed by the Commission	*Amendment*

4. ***in*** Article 5, ***paragraph 11 is replaced by the following***: '11. In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the third party pursuant to paragraph 9 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the third party poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse on a case-by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to the third party without undue delay. ***Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37***.'	4. Article 5 ***is amended as follows*:** ***(a) Paragraph 10 is amended as follows:*** ***'10. Where there is no agreement on the necessary measures referred to in paragraph 9 of this Article or if the third party fails to implement the measures agreed pursuant to paragraph 9 of this Article or undermines the confidentiality of the trade secrets, the data holder may withhold or, as the case may be, suspend the sharing of data identified as trade secrets. The decision of the data holder shall be duly substantiated and provided in writing to the third party without undue delay.';*** ***(b) Paragraph 11 is replaced by the following:*** '11. In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the third party pursuant to paragraph 9 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the third party poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse on a case-by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to the third party without undue delay.;
Justification: The Data Act provides significant *ex-ante* reporting obligations on data holders. These requirements force data holders to notify national competent authorities of their decisions pro-actively even where these do not give rise to a dispute These requirements create unnecessary administrative burden on data holders as they require generating and communicating extensive documentation, which is likely to overwhelm competent authorities, and is unnecessary as these authorities are empowered to request any information they see fit from data holders to	

verify compliance with the Data Act. Repealing these requirements will ease the administrative burden they create for data holders and competent authorities.

Proposal for a regulation **Article 1, para. (4a) NEW**	
Text proposed by the Commission	*Amendment*
New	**4a. Article 8, paragraph 3 is amended as follows:** '3. A data holder shall not discriminate regarding the arrangements for making data available between comparable categories of data recipients, including partner enterprises or linked enterprises of the data holder when making data available.'
Justification: The Data Act provides significant *ex-ante* reporting obligations on data holders. These requirements force data holders to notify national competent authorities of their decisions pro-actively even where these do not give rise to a dispute These requirements create unnecessary administrative burden on data holders as they require generating and communicating extensive documentation, which is likely to overwhelm competent authorities, and is unnecessary as these authorities are empowered to request any information they see fit from data holders to verify compliance with the Data Act. Repealing these requirements will ease the administrative burden they create for data holders and competent authorities.	

8. Transparency obligations under the Data Act

Proposal for amendment

Proposal for a regulation **Article 1, para. (4b) NEW**	
Text proposed by the Commission	*Amendment*
New	**4b. Article 9, paragraph 7 is deleted.**
Justification: The Data Act requires data holders to disclose information setting out basis for the calculation of the compensation required for the provision of data to the data recipients. This requirement forces them to disclose their cost structures, including their cost calculation, upon request, without any threshold and with no handbrake or control. This requirement may not only conflict with contractual obligations of confidentiality, but also EU Competition law, especially where the data holder and the data recipient compete on the same downstream market. Data holders are places in a legal dilemma created by conflicting legal instruments, as they may be	

found in breach of their obligations under the Data Act if they refuse to share this information, and in breach of Competition Law if they do.

These requirements should be repealed to avoid conflict with other legal instruments.

Proposal for a regulation **Article 1, para. (12)**	
Text proposed by the Commission	*Amendment*
12. Article 20 is replaced by the following: 'Article 20 *Compensation for making data available under Chapter V* 1. Data holders shall make available data necessary to respond to a public emergency pursuant to Article 15a(2) free of charge. The public sector body, the Commission, the European Central Bank or the Union body that has received data shall provide public acknowledgement to the data holder if requested by the data holder. 2. The data holder shall be entitled to fair compensation for making data available in compliance with a request made pursuant to Article 15a(3). Such compensation shall cover the technical and organisational costs incurred to comply with the request including, where applicable, the costs of anonymisation, pseudonymisation, aggregation and of technical adaptation, and a reasonable margin. ***Upon request of the public sector body, the Commission, the European Central Bank or the Union body, the data holder shall provide information on the basis for the calculation of the costs and the reasonable margin.*** 3. By way of derogation from paragraph 1 of this Article, a data holder that is a microenterprise or small enterprise may claim compensation for making data available in response to a request under Article 15a(2), according to the conditions set in paragraph 2 of this Article. 4. Data holders shall not be entitled to compensation for making data available in compliance with a request made pursuant to Article 15a(3), where the specific task carried out in the public interest is the production of official statistics	12. Article 20 is replaced by the following: 'Article 20 *Compensation for making data available under Chapter V* 1. Data holders shall make available data necessary to respond to a public emergency pursuant to Article 15a(2) free of charge. The public sector body, the Commission, the European Central Bank or the Union body that has received data shall provide public acknowledgement to the data holder if requested by the data holder. 2. The data holder shall be entitled to fair compensation for making data available in compliance with a request made pursuant to Article 15a(3). Such compensation shall cover the technical and organisational costs incurred to comply with the request including, where applicable, the costs of anonymisation, pseudonymisation, aggregation and of technical adaptation, and a reasonable margin. 3. By way of derogation from paragraph 1 of this Article, a data holder that is a microenterprise or small enterprise may claim compensation for making data available in response to a request under Article 15a(2), according to the conditions set in paragraph 2 of this Article. 4. Data holders shall not be entitled to compensation for making data available in compliance with a request made pursuant to Article 15a(3), where the specific task carried out in the public interest is the production of official statistics and where the purchase of data is not allowed by national law. Member States shall notify the Commission where the purchase of data for the

and where the purchase of data is not allowed by national law. Member States shall notify the Commission where the purchase of data for the production of official statistics is not allowed by national law.’;	production of official statistics is not allowed by national law.’;

Justification:

The Data Act requires data holders to disclose information setting out basis for the calculation of the compensation required for the provision of data to the data recipients. This requirement forces them to disclose their cost structures, including their cost calculation, upon request, without any threshold and with no handbrake or control.

9. Impediment to International data transfer under the Data Act

Proposal for amendment

Proposal for a regulation **Article 1, para. (16), point (ab) NEW**	
Text proposed by the Commission	*Amendment*
New	***(ab) the following point (1a) is inserted:*** ***‘1a. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by any of the measures referred to in Article 45, point (1) and Article 46, point (2), of Regulation (EU) 2016/679.’***

Justification:

The Data Act restricts the transfer of non-personal data to third countries (Art. 32). This article establishes framework for international data transfer which runs parallel the framework laid down in Chapter V of the GDPR, yet largely overlaps with it, creating legal uncertainty and a complex and burdensome administrative compliance requirements for companies operating internationally.

This complexity is reinforced by the lack of a clear definition of “data processing services” and the lack of clarity as to the requirements that such an entity is expected to fulfil pursuant to Article 32.

Allowing data holders to rely on the same mechanisms provided under the GDPR regarding the transfer of personal data to a third country, such as Standard Contractual clauses and technical and organisational measures, should be deemed as satisfying the requirements of Article 32 of the Data Act.

10. Redundancy of the EV data access obligation under RED III

Proposal for amendment

Proposal for a regulation **Article 9a NEW**	
Text proposed by the Commission	*Amendment*
New	***Article 9a***

	Amendment to Directive (EU) 2023/2413 ***In Article 20a, paragraph 3, of Directive (EU) 2023/2413, the second and third subparagraphs are deleted.***

Justification:

The Renewable Energy Directive (RED III) includes a provision making it mandatory for vehicle manufacturers to make available data points about electric vehicle batteries to owners, users and third parties such as energy providers and charging operators (Article 20a(3)).

These requirements create regulatory fragmentation and legal uncertainty, as they invite divergent national rules, and overlap with the requirements of the Data Act's, compromise the economic viability of affordable EVs, and undermine the investment climate for a data-driven economy.

Any data mandated under this provision can be accessed by interested parties pursuant to the provisions of other Regulations, such as the EU Battery Regulation (EUBR), Euro 7, and the Data Act.

II. DATA PROTECTION AND PRIVACY

1. Processing for research purposes

Proposal for amendments

Proposal for a regulation **Article 1, point (b)**	
Text proposed by the Commission	*Amendment*
(b) the following points are added:	(b) the following points are added:
'(32) 'terminal equipment' means terminal equipment as set out in Article 1(1) of Directive 2008/63/EC;	'(32) 'terminal equipment' means terminal equipment as set out in Article 1(1) of Directive 2008/63/EC;
(33) for 'electronic communications networks' the definition of Article 2(1) of Directive (EU) 2018/1972 shall apply;	(33) for 'electronic communications networks' the definition of Article 2(1) of Directive (EU) 2018/1972 shall apply;
(34) 'web browser' means web browser as defined in Article 2(11) of Regulation (EU) 2022/1925;	(34) 'web browser' means web browser as defined in Article 2(11) of Regulation (EU) 2022/1925;
(35) 'media service' means a media service as defined in Article 2(1) of Regulation (EU) 2024/1083;	(35) 'media service' means a media service as defined in Article 2(1) of Regulation (EU) 2024/1083;
(36) 'media service provider' means a media service provider as defined in Article 2(2) of Regulation (EU) 2024/1083;'	(36) 'media service provider' means a media service provider as defined in Article 2(2) of Regulation (EU) 2024/1083;'
(37) 'online interface' means an online interface as defined in Article 3(m) of Regulation (EU) 2022/2065.'	(37) 'online interface' means an online interface as defined in Article 3(m) of Regulation (EU) 2022/2065.'
(38) "scientific research" means any research which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial interest.'	(38) "scientific research" means any research which can also support innovation, such as technological development and demonstration**, *including research carried out by private entities.*** These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial interest.'
Justification: Processing of data for scientific research which support innovation, such as technological development and demonstration, can effectively contribute to promoting innovation and thus to serving the greater societal	

interest, even when it is conducted by private companies for commercial purposes. It should therefore be treated in the same manner as public research.

2. Processing of special categories of personal data for AI

Proposal for amendments

Proposal for a regulation **Article 3, point (a)**	
Text proposed by the Commission	*Amendment*
(b) In paragraph 2, the following points are added: '(k) processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, subject to the conditions referred to in paragraph 5. (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'	(b) In paragraph 2, the following points are added: '(k) processing in the context of **scientific *research, including*** the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, subject to the conditions referred to in paragraph 5. (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: Limiting the exception under Article 9(2)(k) specifically to Artificial Intelligence creates an unnecessary technology-specific restriction, where a technology-neutral approach will support a broader range of innovations that are in the wider societal interest, maximising its potential benefit for the digital economy. This approach ensures that the exception genuinely facilitates innovation by allowing the development and collaboration on new technologies – including, but not limited to, AI.	

Proposal for a regulation **Article 3, para. 3, point (c) NEW**	
Text proposed by the Commission	*Amendment*
New	***(c) paragraph 1 shall be replaced as follows:*** ***'1. Processing of personal data that directly aims to reveal in relation to an identified data subject racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, his or her health status (data concerning health) or sex life or sexual orientation and the processing of genetic data or of biometric data for the purpose of uniquely identifying a natural person shall be prohibited.'***
Justification:	

The processing conditions set out in Article 9(5) significantly curtail the practical utility of the new exception created by the Commission. By requiring controllers to avoid collecting or processing special categories of personal data wherever possible and imposing strict restrictions on the use and sharing of any data that must be processed, the exception becomes largely theoretical. These limitations prevent controllers from effectively leveraging processed data for AI development or collaborative ventures, undermining the very objective of fostering innovation. These restrictions must be lightened in order to allow meaningful use of this data to support innovation.

Proposal for a regulation **Article 3, para. 3, point (b)**	
Text proposed by the Commission	*Amendment*
(b) the following paragraph is added: '5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid **v** the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the control identifies special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such data. If removal of those data requires disproportionate effort, the controller shall in any event effectively protect without undue delay such data ***from being used to produce outputs,*** from being disclosed or otherwise made available to third parties.'	(b) the following paragraph is added: '5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid ~~v~~ the collection and otherwise processing of special categories of personal data, ***where this data directly reveals, in relation to a specific data subject, their racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data and biometric data for the purpose of uniquely identifying a natural person, and data concerning the health, the sex life or sexual orientation of natural person***. Where, despite the implementation of such measures, the control identifies **such** special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such data. If removal of those data requires disproportionate effort, the controller shall in any event effectively protect without undue delay such data from being disclosed or otherwise made available to third parties ***for any purpose other than for the processing referred to in point (k) of paragraph 2***.'
Justification: The processing conditions set out in Article 9(5) significantly curtail the practical utility of the new exception created by the Commission. By requiring controllers to avoid collecting or processing special categories of personal data wherever possible and imposing strict restrictions on the use and sharing of any data that must be processed, the exception becomes largely theoretical. These limitations prevent controllers from effectively leveraging processed data for AI development or collaborative ventures, undermining the very objective of fostering innovation. These restriction must be lightened in order to allow meaningful use of this data to support innovation.	

3. Notification of personal data breach

Proposal for amendment

Proposal for a regulation **Article 3, para. 8, point (ba) NEW**	
Text proposed by the Commission	*Amendment*
New	***(ba) Paragraph 5 is amended as follows:*** ***5. The controller shall document any personal data breaches that are likely to result in a high risk to the rights and freedoms of natural persons, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.***
Justification: The documentation requirements laid down in paragraph 5 place a heavy burden on the industry. In practice, assembling and maintaining comprehensive documentation for every breach – even those unlikely to result in a high risk to individuals – demands significant time and resources, diverting attention from effective incident management and remediation. A more calibrated approach, proportionate and risk-based, would maintain robust protection for individuals while reducing unnecessary administrative complexity, enabling organisations to focus on meaningful security improvements rather than procedural overhead.	

4. Commission empowerment

Proposal for amendment

Proposal for a regulation **Article 3, para. 10**	
Text proposed by the Commission	*Amendment*
10. The following article is added: 'Article 41a ***(1)*** The Commission may adopt implementing acts ***to specify means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities.*** ***(2)*** For the purpose of paragraph 1 the Commission shall***:*** (a) assess the state of the art of available ***techniques;***	10. The following article is added: 'Article 41a **(1)** The Commission may adopt implementing acts ***providing specifications, interpretations or criteria for the application of this Regulation, including with regard to the determination of when data resulting from pseudonymisation no longer constitutes personal data for certain entities.*** ***(2)*** For the purposes of paragraph 1, the Commission shall***, where appropriate:***

(b) develop criteria ***and or*** categories for controllers and recipients to assess the ***risk*** of re-identification ***in relation to typical recipients of data.*** (3) The implementation ***of the means and criteria outlined in an*** implementing ***act*** may be used as an element to demonstrate ***that data cannot lead to reidentification of the*** data ***subjects.*** ***(4)*** The Commission shall closely involve the EDPB in the preparations of the implementing acts. The EPDB shall issue an opinion on the draft implementing acts within a deadline of 8 weeks as of the receipt of the draft from the Commission. ***(5)*** The Implementing Acts shall be adopted in accordance with the examination procedure referred to in Article 93(3).'	(a) assess the state of the art of available ***technologies, data-protection techniques, organisational measures and relevant sectoral practices;*** (b) develop criteria**,** categories ***or methodologies*** for controllers and recipients to assess the ***risks to the rights and freedoms of natural persons, including risks*** of re-identification ***associated with data disclosure, access or reuse;*** ***(c) identify sector-specific circumstances, use-cases or processing operations where tailored guidance, safeguards or interpretative criteria are required to ensure consistent application of this Regulation.*** (3) The implementation ***of the specifications, criteria or methodologies set out*** in implementing ***acts adopted under paragraph 1*** may be used ***by controllers and processors*** as an element to demonstrate ***compliance with this Regulation, including demonstrating that data cannot reasonably be used to re-identify a*** data ***subject.*** (4) The Commission ***is empowered to adopt implementing acts establishing:*** ***(a) codes of conduct pursuant to Article 40 where Union-level harmonisation is necessary; and*** ***(b) certification mechanisms, seals and marks pursuant to Article 42, including detailed certification criteria and the conditions for accreditation of certification bodies.*** ***(5)*** The Commission shall closely involve the European Data Protection Board in the preparation of implementing acts adopted under this Article. The EDPB shall issue an opinion on draft implementing acts within eight weeks of receipt of the draft from the Commission. ***(6)*** The implementing Acts ***referred to in this Article*** shall be adopted in accordance with the examination procedure referred to in Article 93(3).
Justification:	

Limiting the Commission's ability to adopt implementing acts solely to provide specifications on pseudonymisation overlooks other areas of the GDPR where further specification would equally benefit from harmonised guidance. Codes of conduct and certification under Articles 40 and 42 GDPR are examples where additional implementing acts could meaningfully support uniform application. These mechanisms remain underused partly because stakeholders face persistent uncertainty regarding practical requirements and methodologies. Granting the Commission broader empowerment would enable it to address such gaps and promote more consistent interpretation and operationalisation of the GDPR.

5. Terminal Equipment Data

Proposal for amendment

Proposal for a regulation **Article 3, para. (15)**	
Text proposed by the Commission	*Amendment*
15. After Article 88, the following articles are added: ***'Article 88a*** ***Processing of personal data in the terminal equipment of natural persons*** ***(1) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation.*** ***(2) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1).*** ***(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:*** ***(a) carrying out the transmission of an electronic communication over an electronic communication network;*** ***(b) providing a service explicitly requested by the data subject;*** ***(c) creating aggregated information about the usage of an online service to measure the***	***Deleted***

audience of such a service, where it is carried out by the controller of that online service solely for its own use; ***(d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service.*** ***(4) Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply:*** ***(a) the data subject shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means;*** ***(b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject;*** ***(c) if the data subject declines a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.*** ***This paragraph also applies to the subsequent processing of personal data based on consent.*** ***(5) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]***	
Justification: The consent requirement under Article 88a reprises the consent-first mechanism currently applicable under the ePrivacy Directive, and the exceptions to this requirement provided under paragraph 3 are too narrow to help solve the issues raised by the mechanism. The Commission's proposal appears too focused on cookies and does not reflect the reality of the wider Internet of Things (IoT), including connected motor vehicles.	

Proposal for a regulation **Article 4a NEW**	
Text proposed by the Commission	*Amendment*
NEW	***Article 4(a)*** ***Amendment to Directive 2002/58/EC***

	Directive 2002/58/EC is amended as follows: ***1. In Article 5, the following paragraphs are added:*** ***'4. Paragraph 3 shall not apply where the storing of information, or the gaining of access to information already stored in the terminal equipment of a user or subscriber, is strictly necessary for processing operations that demonstrably create, or have the potential to create, significant societal benefits, in accordance with paragraph 5.'*** ***5. Processing under paragraph 4 shall only apply where the storing of or access to information in terminal equipment is strictly necessary to further a purpose with the potential to create societal benefit.*** ***For the purposes of this paragraph, "societal benefit" includes, inter alia:*** ***(a) road safety, transport safety, and accident prevention, including the operation, maintenance, and improvement of connected vehicles and mobility systems;*** ***(b) public health, epidemiological monitoring, and health-related research;*** ***(c) cybersecurity, detection and remediation of vulnerabilities, and resilience of critical infrastructure;*** ***(d) environmental protection, climate-related monitoring, and energy efficiency;*** ***(e) scientific research and innovation activities with broad societal relevance;*** ***(f) other purposes listed in implementing acts adopted under Article 5(3b).'*** ***'6. The Commission is empowered to adopt implementing acts establishing and regularly updating a Unionwide list of processing operations that qualify as societal benefit purposes under paragraph 5.*** ***7. Paragraph 3 shall not prevent the storage of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user, insofar as such storage or access is strictly necessary for the purpose of complying with an obligation laid down in Union or Member State law***

	2. After article 5, the following article is added: ***Article 5a*** ***Exercised of the delegation*** ***1. The implementing acts referred to in article 5 shall specify:*** ***(a) categories of processing operations considered to generate significant societal benefits;*** ***(b) minimum safeguards and technical standards required for such operations;*** ***(c) conditions for inclusion or removal of processing operations from the list.*** ***2. In preparing these implementing acts, the Commission shall take into account:*** ***(a) the expected societal benefits, including in the fields of safety, public health, environment, scientific research, innovation, and cybersecurity;*** ***(b) risks to fundamental rights and freedoms;*** ***(c) the availability of less intrusive means;*** ***(d) evidence from scientific, industrial, and regulatory stakeholders.*** ***3. The Commission shall consult the European Data Protection Board and the European Union Agency for Cybersecurity (ENISA), which shall issue an opinion within eight weeks of receiving a draft implementing act.*** ***4. The implementing acts referred to in this Article shall be adopted in accordance with the examination procedure laid down in Article 14a(2).'*** ***3. Article 14a is replaced by the following:*** ***'Article 14a*** ***Committee procedure*** ***1. The Commission shall be assisted by a committee within the meaning of Regulation (EU) No 182/2011.*** ***2. Where reference is made to this paragraph, the examination procedure under Article 5 of Regulation (EU) No 182/2011 shall apply.'***
Justification:	

Strict reliance on consent for any access to or storage of information on terminal equipment has led to legal uncertainty, consent fatigue and poorly informed choices, and a structural disincentive for European companies to deploy socially valuable, privacy-respecting services.

Introducing a carefully framed, purpose-based exception system in Article 5(3) of the ePrivacy Directive would improve protection for individuals because processing would occur only where objectively justified and regulated, rather than hidden behind formalistic consent flows. It would also provide legal certainty for controllers wishing to deploy privacy-respecting technologies for socially valuable services, who currently face legal risk or are forced into ineffective consent mechanisms that neither serve users nor innovation.

6. Principle of proportionality

Proposal for amendment

Proposal for a regulation **Article 3, para. 2a NEW**	
Text proposed by the Commission	*Amendment*
New	***(2a) In Article 5, the following paragraph 3, is added:*** ***(3) The principles of this Regulation for the protection of personal data shall be interpreted in such a way that the requirements of this Regulation are proportionate to the purpose pursued in each case and, in particular, take into account the varying likelihood and severity of the risk that a data processing operation poses to the rights and freedoms of natural persons (risk-based approach). Measures for the protection of personal data shall be balanced in an appropriate manner with the interests or the fundamental rights and freedoms of persons other than the data subject.***

Justification:

A recurring challenge in the application of the GDPR is the increasingly strict interpretation adopted by courts and supervisory authorities, which often places disproportionate burdens on data controllers. While the Regulation aims to strike a balance between protecting individuals' rights and enabling lawful data use, its practical enforcement has at times shifted this balance, resulting in overly rigid compliance expectations that go beyond what is necessary for achieving GDPR's objectives. This trend risks creating legal uncertainty, discouraging innovation and complicating the deployment of data-driven technologies across the European Union.

To address this issue, embedding proportionality alongside the existing principles relating to the processing of personal data in the GDPR would reinforce the need for interpretation and enforcement that respects the balance between individual rights and legitimate organisational interests.

III. Cybersecurity

1. Definition of 'Sector'

Proposal for amendment

Proposal for a regulation **Article 6, para. 1a (NEW)**	
Text proposed by the Commission	*Amendment*
New	***1a. In Article 6, the following point (38a) is added:*** ***'(38a) 'Sector' means all manufacturing, trading or service enterprises engaged in the same principal activity;'***
Justification: A definition of the concept of 'sector' should be included in Directive (EU) 2022/2555 to ensure that cybersecurity rules apply not just to individual entities but to coherent groups of economic actors sharing similar risk profiles and systemic functions (e.g., energy, health, transport). This supports consistent identification of critical economic areas, enables proportionate risk management and supervision, and avoids gaps or overlaps in obligations across interconnected operators whose collective disruption could impact the security of network and information systems.	

2. Harmonisation of reporting obligations of the cybersecurity framework

Proposal for amendment

Proposal for a regulation **Article 6, para. (1)**	
Text proposed by the Commission	*Amendment*
1. The following Article 23a is added: 'Article 23a *Single-entry point for incident reporting* (1) ENISA shall develop and maintain a single-entry point to support the obligation to report incidents and related events under the Union legal acts where those Union legal acts provide so ('single-entry point'). Without prejudice to Article 16 of Regulation (EU) 2024/2847 of the European Parliament and of the Council, ENISA may ensure that the single-entry point builds on the	1. The following Article 23a is added: 'Article 23a *Single-entry point for incident reporting* (1) ENISA shall develop and maintain a single-entry point to support the obligation to report incidents and related events under the Union legal acts where those Union legal acts provide so ('single-entry point'). Without prejudice to Article 16 of Regulation (EU) 2024/2847 of the European Parliament and of the Council, ENISA may ensure that the single-entry point builds on the

single reporting platform established under that Regulation.	single reporting platform established under that Regulation.
(2) ENISA shall take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the single-entry point and the information submitted or disseminated via the single-entry point. ENISA shall take into account the sensitivity of information submitted or disseminated pursuant to the Union legal acts referred to in paragraph (1) and ensure that competent authorities under those Union legal acts have access to and process the information as required under those Union legal acts.	***(1a) Within [18] months from the entry into force of this Regulation, ENISA shall define the single list of information required for incident notification, provided for in Article 23a(1).***
	(1b) Member States shall not impose competing notification obligations where there is already an obligation to notify incidents or vulnerabilities related to activities or products under Union law.
	(2) ENISA shall take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the single-entry point and the information submitted or disseminated via the single-entry point. ENISA shall take into account the sensitivity of information submitted or disseminated pursuant to the Union legal acts referred to in paragraph (1) and ensure that competent authorities under those Union legal acts have access to and process the information as required under those Union legal acts.
(3) ENISA shall provide and implement the specifications on the technical, operational and organisational measures regarding the establishment, maintenance and secure operation of the single-entry point. ENISA shall develop the specifications in cooperation with the Commission, the CSIRTs network and the competent authorities under the Union legal acts referred to in paragraph (1). The specifications shall ensure that:	(3) ENISA shall provide and implement the specifications on the technical, operational and organisational measures regarding the establishment, maintenance and secure operation of the single-entry point. ENISA shall develop the specifications in cooperation with the Commission, the CSIRTs network and the competent authorities under the Union legal acts referred to in paragraph (1). The specifications shall ensure that:
(a) the necessary capability for interoperability with regard to other relevant reporting obligations referred to in paragraph (1) is ensured;	(a) the necessary capability for interoperability with regard to other relevant reporting obligations referred to in paragraph (1) is ensured;
(b) technical arrangements for the relevant entities and authorities under the Union legal acts referred to in paragraph (1) to access, submit , retrieve, transmit or otherwise process information from the single-entry point, are in place and, provide technical protocols and tools that allow the entities and authorities to further process the receive information within their systems;	(b) technical arrangements for the relevant entities and authorities under the Union legal acts referred to in paragraph (1) to access, submit , retrieve, transmit or otherwise process information from the single-entry point, are in place and, provide technical protocols and tools that allow the entities and authorities to further process the receive information within their systems;
(c) the specificities of the incident reporting requirements set out under the Union legal acts referred to in paragraph (1) are duly taken into account;	
(d) where relevant, the single-entry point is interoperable and compatible with European Business Wallets referred to in *[Proposal for a Regulation: Insert title of the proposal]* and that the European Business Wallets can	

be used at least to identify and authenticate entities using the single-entry point; (e) entities using the single-entry point can retrieve and supplement information that they have previously submitted via the single-entry point; (f) a single notification of information submitted by an entity via the single-entry point can be used to fulfil reporting obligations as set out under any of the other Union legal acts which provide for incident reporting to the single-entry point. (4) Unless provided for in the Union legal acts referred to in paragraph (1) of this, ENISA **and national authorities** shall not have access to the notifications submitted through the single-entry point. (5) Within [18] months from the entry into force of this Regulation, ENISA shall pilot the functioning of the single-entry point for each added Union legal act, including testing that takes into account the specificities and requirements for the notifications set out by each respective Union legal act, and after consulting the Commission and the relevant competent authorities under the respective Union legal acts. ENISA shall enable the notification of incidents under each Union legal act referred to in paragraph (1) only after piloting the functioning and after the Commission published a notice pursuant to paragraph 6. (6) The Commission shall, in cooperation with ENISA, assess the proper functioning, reliability, integrity and confidentiality of the single-entry point. When the Commission, after consultation of the CSIRTs network and the competent authorities under the Union legal acts referred to in paragraph 1, finds that the single-entry point ensures the proper functioning, reliability, integrity and confidentiality, it shall publish a notice to that effect in the Official Journal of the European Union. (7) Where the Commission finds in its assessment that the single-entry point does not ensure the proper functioning, reliability, integrity or confidentiality, ENISA shall take, in cooperation with the Commission and without undue delay,	(c) the specificities of the incident reporting requirements set out under the Union legal acts referred to in paragraph (1) are duly taken into account; (d) where relevant, the single-entry point is interoperable and compatible with European Business Wallets referred to in *[Proposal for a Regulation: Insert title of the proposal]* and that the European Business Wallets can be used at least to identify and authenticate entities using the single-entry point; (e) entities using the single-entry point can retrieve and supplement information that they have previously submitted via the single-entry point; (f) a single notification of information submitted by an entity via the single-entry point can be used to fulfil reporting obligations as set out under any of the other Union legal acts which provide for incident reporting to the single-entry point. (4) Unless provided for in the Union legal acts referred to in paragraph (1) of this, ENISA shall not have access to the notifications submitted through the single-entry point. (5) Within [18] months from the entry into force of this Regulation, ENISA shall pilot the functioning of the single-entry point for each added Union legal act, including testing that takes into account the specificities and requirements for the notifications set out by each respective Union legal act, and after consulting the Commission and the relevant competent authorities under the respective Union legal acts. ENISA shall enable the notification of incidents under each Union legal act referred to in paragraph (1) only after piloting the functioning and after the Commission published a notice pursuant to paragraph 6. (6) The Commission shall, in cooperation with ENISA, assess the proper functioning, reliability, integrity and confidentiality of the single-entry point. When the Commission, after consultation of the CSIRTs network and the competent authorities under the Union legal acts referred to in paragraph 1, finds that the single-entry point ensures the proper functioning, reliability,

all necessary corrective measures to ensure the proper functioning, reliability, integrity or confidentiality without delay and inform the Commission of the results. Thereafter, the Commission shall reassess the proper functioning, reliability, integrity or confidentiality of the single-entry point and shall publish a notice in accordance with paragraph 6.'	integrity and confidentiality, it shall publish a notice to that effect in the Official Journal of the European Union. (7) Where the Commission finds in its assessment that the single-entry point does not ensure the proper functioning, reliability, integrity or confidentiality, ENISA shall take, in cooperation with the Commission and without undue delay, all necessary corrective measures to ensure the proper functioning, reliability, integrity or confidentiality without delay and inform the Commission of the results. Thereafter, the Commission shall reassess the proper functioning, reliability, integrity or confidentiality of the single-entry point and shall publish a notice in accordance with paragraph 6.'

Justification:

Discrepancies in the scope, rules and processes laid down in various EU legal instruments that require reporting incidents and data breach create a significant burden for stakeholders. NIS 2 Directive, the Cyber Resilience Act (CRA), the Digital Operational Resilience Act (DORA) and the GDPR lay down different procedures, different timelines, and appoint different reporting authorities for the reporting of relevant incidents and breach. This diverts critical resources from operational response to administrative tasks, undermining the very security these regulations aim to enhance.

To support harmonisation, ENISA and the European Commission should be required to define a single list of information required for incident notification, and Member States should be prohibited from imposing concurrent notification obligations where there is already an obligation to notify incidents or vulnerabilities relating to activities or products, in order to avoid the accumulation of notification obligations.

Proposal for a regulation **Article 9a (NEW)**	
Text proposed by the Commission	*Amendment*
New	***Article 9a*** ***Amendment to Regulation (EU) 2024/2847*** ***Article 14 of Regulation (EU) 2024/2847 is amended as follows:*** ***1. Paragraph 1 is replaced by the following:*** ***'1. A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA, via the single-entry point***

	established pursuant to Article 23a of Directive (EU) 2022/2555. **2.** ***Paragraph 3 is replaced by the following:*** ***'3. A manufacturer shall notify any severe incident having an impact on the security of the product with digital elements that it becomes aware of to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA, via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555.*** **3.** ***Paragraph 6 is replaced by the following:*** ***'6. ENISA shall prepare and transmit to the Commission a proposal for a common template for notifying an actively exploited vulnerability contained in a product with digital elements, pursuant to paragraph 1, and any severe incident having an impact on the security of a product with digital elements, pursuant to paragraph 3. The proposal shall be submitted to the Commission within [OP date = nine months of the entry into application of this Regulation]. The Commission. after due consideration, reviews it as necessary and is empowered to adopt it by way of an implementing act, pursuant to paragraph 10.*** **4.** ***Paragraph 7 is replaced by the following:*** ***'7. The template referred to in paragraph 6 shall be reviewed at least every three years and updated where necessary. ENISA shall submit its assessment and possible proposal for updates to the Commission in due time. The Commission. after due consideration, reviews it as necessary and is empowered to adopt any updates following the procedure in paragraph 6.'***
Justification: Discrepancies in the scope, rules and processes laid down in various EU legal instruments that require reporting incidents and data breach create a significant burden for stakeholders. NIS 2 Directive, the Cyber Resilience Act (CRA), the Digital Operational Resilience Act (DORA) and the GDPR lay down different procedures, different timelines, and different reporting authorities, diverting critical resources from operational response to	

administrative tasks. To support simplification of cybersecurity incident reporting, EU-wide standard templates should be developed and reporting criteria defined that would apply to all Member States, to avoid diverging requirements at national level.

3. Enforcement of Cybersecurity measures based on risk

Proposal for amendment

Proposal for a regulation **Article 6, para. 1b (NEW)**	
Text proposed by the Commission	*Amendment*
New	***1b. In Article 2, the following paragraph 8a is added :*** ***'8a.With regard to paragraph 1, Member States shall take into account the degree of independence that an entity enjoys from its partners and related undertakings in terms of the network and information systems it uses to provide its services and in terms of the services it provides and, where appropriate, consider that such an entity does not constitute a medium-sized enterprise within the meaning of Article 2 of the Annex to Recommendation 2003/361/EC or does not exceed the thresholds applicable to a medium-sized enterprise set out in paragraph 1 of that Article.'***
Justification: NIS 2 applies cybersecurity obligations to all of an entity's information systems, regardless of their relevance to critical activities. This forces organisations to treat low-risk or ancillary systems as mission-critical, increasing compliance and audit costs without a matching security benefit and disproportionately burdening smaller, less complex entities. Where an entity operates independently, as recognised in Recital 16, Member States should assess it on the basis of its own data and disregard disproportionate group-level consolidation to avoid unfairly classifying it as a medium-sized enterprise.	

ABOUT THE EU AUTOMOBILE INDUSTRY

- 13.6 million Europeans work in the auto industry (directly and indirectly), accounting for 6.9% of all EU jobs
- 8.1% of EU manufacturing jobs – some 2.5 million – are in the automotive sector
- Motor vehicles are responsible for €414.7 billion of tax revenue for governments across key European markets
- The automobile industry generates a trade surplus of €93.9 billion for the European Union
- The turnover generated by the auto industry represents over 8% of the EU's GDP
- Investing €84.6 billion in R&D per year, automotive is Europe's largest private contributor to innovation, accounting for 34% of the EU total

ACEA REPRESENTS EUROPE'S 17 MAJOR CAR, VAN, TRUCK AND BUS MANUFACTURERS

ACEA
European Automobile
Manufacturers' Association
+32 2 732 55 50
info@acea.auto
www.acea.auto

x.com/ACEA_auto

linkedin.com/company/acea

youtube.com/c/ACEAauto