GDPR in Digital Omnibus, Nordic Comments

Text Location	Commission Proposal	Council Compromise Text 21.05	Nordic Business Federations, Suggestion	Nordic Business Federations, Comment
Article 3, paragraph 1, point (a) (amending GDPR Article 4(1))	1.Article 4 is amended as follows: (a)in point 1, the following sentences are added: 'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'	~~1.Article 4 is amended as follows:~~ ~~(a)in point 1, the following sentences are added:~~ ~~'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'~~	Keep the Commission proposal or: **'Regulation (EU) 2016/679 shall not apply to the processing of personal data, including sensitive personal data, where:** **(a) the processing is merely transitory in nature [or for a limited period of time not exceeding…]; and** **(b) the processing is for a purpose that is unrelated to the data subject as an identified or identifiable natural person; and** **(c) appropriate technical and/or organisational safeguards are in place to prevent any use of the data for a purpose related to the data subject as an identified or identifiable natural person up to the point when the data are irreversibly anonymised or erased.** **2. Data shall not be considered as personal data within the meaning of Regulation (EU) 2016/679 and other Union and national law referring to or relying on the notion of personal data within the meaning of Regulation (EU) 2016/679 insofar as:** **(a) the data relate primarily to an entity other than a natural person, such as an enterprise or an object, and the data subject is associated with that entity exclusively as owner, employee**	The broad definition of personal data in Article 4(1) of the GDPR severely impacts business R&D, including AI development. True anonymisation is difficult or even impossible to achieve and often reduces the quality and usefulness of data. To be innovative, competitive, and promote more AI development and use, companies need to be able to extract aggregated knowledge at group level. Thus Commission's proposal to streamline the definition of personal data is a true gamechanger, however the current changes do not fully solve the issues. Instead, we propose to add an exception where non-personal use of personal data is exempted.

			or in a similar function; and **(b) processing of the data is for a purpose that is not specifically related to the data subject as an identified or identifiable natural person; and** **(c) appropriate technical and/or organisational safeguards are in place to prevent any use of the data for a purpose specifically related to the data subject as an identified or identifiable natural person.'**	
Article 3, paragraph 1, point (b) (adding definitions to GDPR)	(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.'	Article 4 is amended as follows: (b) the following points are added: '(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~~ **conducted in an autonomous and independent manner**, ~~be carried out~~ with the aim of contributing to the growth of society's general knowledge and wellbeing, **generating new or complementing existing scientific knowledge, following a methodological and systematic approach consistent with standards of the relevant scientific field**, **including** ~~and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial~~	(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'~~**, testing or development activity regarding AI systems or AI models prior to their being placed on the market or put into service or the** aim to further a commercial interest.'	It is vital to improve innovation that the Commission's proposal is kept as it enables companies in the EU to process personal data in certain types of R&D. To promote innovation and the developing of AI it is crucial that the definition added corresponds to AI Act article 2, both point 6 and 8: 6. This Regulation does not apply to AI systems or AI models, including their output, specifically developed and put into service for the sole purpose of scientific research and development. 8. This Regulation does not apply to any research, testing or development activity regarding AI systems or AI models prior to their being placed on the market or put into service. Such activities shall be conducted in accordance with applicable Union law. Testing in real world conditions shall not be covered by that exclusion.

		~~interest,~~ **and producing verifiable and transparent results.'**		
Article 3 paragraph 2 (replacing GDPR Article 5 (1)(b))	Article 5 (1)(b) is replaced by the following: 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), be considered to be compatible with the initial purposes, independent of the conditions of Article 6(4) of this Regulation, ('purpose limitation');'	Article 5 (1)(b) is replaced by the following: 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, **subject to the application of appropriate safeguards** in accordance with Article 89(1), be considered to be compatible with the initial purposes, independent of the conditions of Article 6(4) of this Regulation, ('purpose limitation');'	Article 5 (1)(b) is replaced by the following: 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), be considered to be compatible with the initial purposes, independent of the conditions of Article 6(4) of this Regulation, ('purpose limitation');'	Keep the Commission proposal. Removing the Article 6(4) compatibility test for research, archiving, and statistical further processing eliminates a frequent point of friction.
Article 3, paragraph 3, point (a) (introducing GDPR Article 9. 2 (k) and (l) and 9.5)	Article 9 is amended as follows: (a) 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)the following paragraph is added:	Article 9 is amended as follows: (a) in paragraph 2, the following points are added: '(k) **incidental and residual** 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 **as referred to in Regulation (EU) 2024/1689,** 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 **one-to-one** verification is under the sole control of the data subject and, **where applicable,**	Article 9 is amended as follows: (a) 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)the following paragraph is added:	Keep Commission's proposal together with new 88c. Processing of special categories of personal data (SCD), art 9 (i.e. racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, health, or sex life or sexual orientation, as well as genetic or biometric data processed for the purpose of uniquely identifying an individual). Processing of SCD is prohibited, unless any of the exemptions in Art. 9 GDPR is applicable

	'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 controller 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.'	**subject to appropriate safeguards to protect the fundamental rights and the interests of the data subject, as laid down in Union law or Member State law, in accordance with paragraph 4 of this Article.'** (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 controller identifies special categories of personal data that are **incidentally and residually involved** in the datasets used for training, testing or validation or in the AI system ~~or AI model~~, the controller shall ~~remove~~ **erase** such data. If ~~removal~~ **erase** of those data proves to be **impossible or** requires **manifestly** disproportionate effort, the controller shall ~~in any event effectively protect,~~ without undue delay **and in any event, effectively protect** such data from being **further processed or processed for other purposes**, used to produce outputs, ~~from being~~ disclosed or otherwise made available to third parties. **The controller shall establish a process of regular verification and assessment of the effectiveness of the measures implemented and shall comprehensively document those**	'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 controller 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.'	There is no legal basis similar to the legitimate interest to process SCD, which puts an unnecessary limit on the processing of such personal data where the processing would be needed eg. to avoid bias and promote representativeness. Processing of special category of personal data for technology, AI systems and models' development is currently extremely challenging. For large data sets it is impossible to rely on consent, and there are rarely other legal bases available. Large language models are developed based on enormous data sets collected by scraping the internet for content amongst other data sets. For development of AI-models and processing of very large data sets it is impossible to rely on consent, and therefore it is currently nearly impossible for commercial businesses to process special category data – even if highly de-identified – to train systems and models. Also, delete the requirement in points (g) and (i) that the substantial public interest (public-health basis) must be grounded in a specific Union or Member State law. The restrictions for processing SCD should pertain solely to data processed with the intent of revealing such data. It should also be clarified that "revealing"

		measures and the results of the assessments throughout the life cycle of the AI system.'		does not mean the existence of any theoretical possibility of identifying a sensitive trait. A suggestion would be to add a legal exemption for processing of special category data on a de-identified/non personal use of personal data, similar to the legitimate interest's basis in Art. 6 (1) (f) GDPR, to Art. 9 GDPR. An alternative could be a new and stricter legitimate interest assessment for special category of personal data.
Article 3, paragraph 4 (replacing GDPR article 12, paragraph 5)	In Article 12, paragraph 5 is replaced by the following: '5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character or also, for requests under Article 15 because the data subject abuses the rights conferred by this regulation for purposes other than the protection of their data, the controller may either: (a)charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action	In Article 12, paragraph 5 is replaced by the following: '5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character or ~~also, for requests under Article 15 because~~ **where an abusive intention on the part** of the data subject abuses the rights conferred by this ~~regulation for purposes other than the protection of their data~~ **submitting those requests can be demonstrated**, the controller may either: (a) charge a reasonable fee ~~taking into account~~ **proportionate to** the administrative costs of providing the	In Article 12, paragraph 5 is replaced by the following: '5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character or also, for requests under Article 15 because the data subject abuses the rights conferred by this regulation for purposes other than the protection of their data, the controller may either: (a)charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action	Too many data access requests today are spent harassing companies, limiting their available time to spend on protecting high risk processing activities. Letting the data controller bear the burden of proof that a request is abusing the rights conferred by the GDPR for purposes other than protection of their data, risks undermining the intention of the suggested improvement.

	requested; or (b)refuse to act on the request. The controller shall bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive.'	information or communication or taking the action requested; or (b) refuse to act on the **request and inform the data subject of the reasons thereof**. The controller shall bear the burden of demonstrating**, in the light of all the relevant circumstances of the case**, that the request is manifestly unfounded ~~or that there are reasonable grounds to believe that it is excessive.~~'	requested; or (b)refuse to act on the request. ~~The controller shall bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive.'~~	
Article 3, paragraph 5 (replacing GDPR article 13, paragraph 4	In Article 13, paragraph 4 is replaced by the following: 'Paragraphs 1, 2 and 3 shall not apply where the personal data have been collected in the context of a clear and circumscribed relationship between data subjects and a controller exercising an activity that is not data-intensive and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1, unless the controller transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35.'	In Article 13, paragraph 4 is replaced by the following: 'Paragraphs 1, 2 and 3 shall not apply ~~where the personal data have been collected in the context of a clear and circumscribed relationship between data subjects and a controller exercising an activity that is not data-intensive~~ and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1 **and the personal data are collected in the context of a direct and clearly circumscribed relationship between data subjects and a controller exercising an activity that is not likely to result in a high risk to the rights and freedoms of data subjects nor involve complex processing operations, the processing of large amounts of personal data, special categories of personal data, or personal data relating to criminal convictions and offences.**	In Article 13, paragraph 4 is replaced by the following: 'Paragraphs 1, 2 and 3 shall not apply where the personal data have been collected in the context of a clear and circumscribed relationship between data subjects and a controller exercising an activity that is not data-intensive and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1, ~~unless the controller transmits the data to other recipients or categories of recipients, transfers the data to a third country,~~ carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35. '	The Commission's proposal is very close to being an excellent burden reduction for companies that are also affected by the proposed amendment to art. 30 in the SMC Omnibus. However, the derogation loses its effect when the information requirement still applies when data is transmitted to other recipients or transferred to a third country, as almost all controllers are outsourcing part of the processing to data processors through the use of third-party IT-systems. Thus, for the derogation to apply in practice, we propose to remove the derogation to still inform on transmission to third party and third country transfers.

		The first subparagraph shall not apply where~~, unless~~ the controller **intends to process the data collected from the data subject for other purposes,** transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35.'		
Article 3, paragraph 6 (adding a new paragraph 5 to GDPR article 13)	In Article 13, paragraph 5 is added: 'When the processing takes place for scientific research purposes and the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing, the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available. '	In Article 13, paragraph 5 is added: 'When the **further** processing takes place for scientific research purposes **by the same controller and where and insofar as** ~~and~~ the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort ~~subject to the conditions and safeguards referred to in Article 89(1)~~ or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that **further** processing, **subject to the conditions and safeguards referred to in Article 89(1),** the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and	In Article 13, paragraph 5 is added: 'When the processing takes place for scientific research purposes and the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing, the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available. '	The commission proposal is a simplification and important for competitiveness. Adding the derogation in art. 14(5b) to art. 13 is good, however to ensure proper use of the derogation, it is necessary to be clear on what level of effort is disproportionate, especially in relation to obtaining the data subjects contact information, which can be a very burdensome task when doing scientific research, as it will often involve information about a substantial amount of data subjects.

		legitimate interests, including making the information publicly available. '		
Article 3, paragraph 7 (amending GDPR Article 22)	'7. In Article 22, paragraphs 1 and 2 are replaced by the following: '1. A decision which produces legal effects for a data subject or similarly significantly affects him or her may be based solely on automated processing, including profiling, only where that decision: (a)is necessary for entering into, or performance of, a contract between the data subject and a data controller regardless of whether the decision could be taken otherwise than by solely automated means; (b)is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c)is based on the data subject's explicit consent.'	'7. ~~In~~ Article 22~~, paragraphs 1 and 2 are~~ **is** replaced by the following: '1. ~~A decision which produces legal effects for a~~ **The** data subject ~~or similarly significantly affects him or her may be~~ **shall have the right not to be subject to a decision** based solely on automated processing, including profiling, ~~only where that decision~~ **which produces legal effects concerning him or her or similarly significantly affects him or her, unless such processing**: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller ~~regardless of whether the decision could be taken otherwise than by solely automated means~~; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent. **2. In the cases referred to in points (a) and (c) of paragraph 1, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the**	'7. In Article 22, paragraphs 1 and 2 are replaced by the following: '1. A decision which produces legal effects for a data subject or similarly significantly affects him or her may be based solely on automated processing, including profiling, only where that decision: (a)is necessary for entering into, or performance of, a contract between the data subject and a data controller regardless of whether the decision could be taken otherwise than by solely automated means; (b)is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c)is based on the data subject's explicit consent.'	Keep the Commission proposal. The redraft from a "right not to be subject to" formulation into an authorisation framework with three explicit bases aligns the text with how modern services operate. The three lawful bases are appropriate; the Article 22(3) safeguards (human intervention, right to express a view, right to contest) remain unchanged and continue to do the substantive protective work. Article 22(1) GDPR prohibits automated individual decision-making in cases where the decision produces legal effects concerning a natural person or otherwise significantly affects them. However, the prohibition does not apply where automated decision-making is expressly permitted, for example, under other EU law or the national legislation of a Member State. However, AI systems are increasingly responsible for automated decision-making across various sectors. Annex III of the EU AI Act lists high-risk AI use cases. One such high-risk but still permissible use case concerns the assessment and decision-making related to essential private and public

		part of the controller, to express his or her point of view and to contest the decision. **3. Decisions referred to in paragraph 1 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.'**		services and benefits. Ambiguous requirements lead to legal uncertainty for companies engaged in AI development and usage as well as slow down AI pilots in the public sector and by authorities. The Commission proposal is in the right direction but more needs to be done to align with AI Act and support AI-use and innovation.
Recital 31 (GDPR Article 24)	'When the controller, in the light of the risk-based approach which informs the scalability of the obligations under this Regulation, is balancing the legitimate interest pursued by the controller or a third party and the interests, rights and freedoms of the data subject, consideration should be given to whether the interest pursued by the controller is beneficial for the data subject and society at large, which may for instance be the case where the processing of personal data is necessary for detecting and removing bias, thereby protecting data subjects from discrimination, or where the processing of personal data is aiming at ensuring accurate and safe outputs for a beneficial use, such as to improve accessibility to certain services. Consideration should also, among others, be given to reasonable expectations of the data subject based on their relationship with the controller,	~~'When the controller, in the light of the risk-based approach which informs the scalability of the obligations under this Regulation, is balancing the legitimate interest pursued by the controller or a third party and the interests, rights and freedoms of the data subject, consideration should be given to whether the interest pursued by the controller is beneficial for the data subject and society at large, which may for instance be the case where the processing of personal data is necessary for detecting and removing bias, thereby protecting data subjects from discrimination, or where the processing of personal data is aiming at ensuring accurate and safe outputs for a beneficial use, such as to improve accessibility to certain services. Consideration should also, among others, be given to reasonable expectations of the data subject based on their relationship with the controller,~~	'When the controller, in the light of the risk-based approach which informs the scalability of the obligations under this Regulation, is balancing the legitimate interest pursued by the controller or a third party and the interests, rights and freedoms of the data subject, consideration should be given to whether the interest pursued by the controller is beneficial for the data subject and society at large, which may for instance be the case where the processing of personal data is necessary for detecting and removing bias, thereby protecting data subjects from discrimination, or where the processing of personal data is aiming at ensuring accurate and safe outputs for a beneficial use, such as to improve accessibility to certain services. ~~Consideration should also, among others, be given to reasonable expectations of the data subject based on their relationship with the controller,~~	The proposal adds minor simplification to GDPR as addresses documentation requirements in the legitimate interest impact assessment and provides legal certainty for certain processing purposes that is often related to AI such as bias detection. The Nordic Business Federations hoped to see an increasing focus in the Digital Omnibus on reducing administrative burdens in accordance with the risk based approach and principle of proportionality. Documentation requirements after articles 24 and 5 should emphasise and acknowledge that all accountability measures (documentation requirements) taken by the controller should be risk based, also forcing data protection authorities to take this into account for auditing and guidance.

	appropriate safeguards to minimise the impact on data subjects' rights such as providing enhanced transparency to data subjects, providing an unconditional right to object to the processing of their personal data, respecting technical indications embedded in a service limiting the use of data for AI development by third parties, the use of other state of the art privacy preserving techniques for AI training and appropriate technical measures to effectively minimise risks resulting, for example, from regurgitation, data leakage and other intended or foreseeable actions.'	~~appropriate safeguards to minimise the impact on data subjects' rights such as providing enhanced transparency to data subjects, providing an unconditional right to object to the processing of their personal data, respecting technical indications embedded in a service limiting the use of data for AI development by third parties, the use of other state of the art privacy preserving techniques for AI training and appropriate technical measures to effectively minimise risks resulting, for example, from regurgitation, data leakage and other intended or foreseeable actions.'~~	~~appropriate safeguards to minimise the impact on data subjects' rights such as providing enhanced transparency to data subjects, providing an unconditional right to object to the processing of their personal data, respecting technical indications embedded in a service limiting the use of data for AI development by third parties, the use of other state of the art privacy preserving techniques for AI training and appropriate technical measures to effectively minimise risks resulting, for example, from regurgitation, data leakage and other intended or foreseeable actions.~~'	We agree that there should always be a legal basis for processing personal data or that data should be erased in accordance with the principle of storage limitation. However, it should be disproportionate in many circumstances to e.g. require retention policies, logs and documentation of all legitimate interests to ensure compliance with articles 24, cf. 6(1)(f) and 5(2). Rather it should be sufficient for most processing activities – especially low and medium risk.
(amending GDPR article 25, para 1 and 2)		**1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, with particular regard to the lists referred to in Article 35(4) and (5), the controller and the processor shall, both at the time of the determination of the means for processing and at the time of the processing itself as applicable, implement, in an effective manner, appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data**	1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, with particular regard to the lists referred to in Article 35(4) and (5), the controller and the processor shall, both at the time of the determination of the means for processing and at the time of the processing itself as applicable, implement, in an effective manner, appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, to integrate the necessary	This is a simplification for any customer using IT-systems developed by a third party (processor's systems). The Nordic Business Federations propose to keep the Councils proposal, which we understand as an attempt to strike a practical balance between the allocation of responsibility of the data controller and data processor. In the current GDPR, responsibility for ensuring data protection by design and default is allocated to the controller alone. However, in practice, data controllers are usually customers that buy in on already existing software and, in reality, have limited capability to determine the content of the default

		minimization, to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. **2. The controller and the processor shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.**	safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2. The controller and the processor shall implement appropriate technical and organizational measures ~~for ensuring~~ **to ensure** that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.	settings, including privacy settings and – depending on the nature of the system – to redesign the system. Thus, placing responsibility on the data processor to also implement data protection by design and default is a welcome change. Furthermore, we understand the reference to positive and negative DPIA lists as a means of using the risk based nature of GDPR to underline the importance of data protection by design and default in high risk processing operations.
Article 3, paragraph 8, point (a) (amending GDPR Article 33)	8. Article 33 is amended as follows: (a)paragraph 1 is replaced by the following: '1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 96 hours after having become aware of it, notify the personal data breach via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555 to the supervisory authority	Article 33 is amended as follows: (a)paragraph 1 is replaced by the following: '1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than ~~96~~ **72** hours after having become aware of it, notify the personal data breach via the ~~single-entry~~ **national entry** point established pursuant to Article ~~23a~~ **23b** of Directive (EU) 2022/2555 to the	Article 33 is amended as follows: (a)paragraph 1 is replaced by the following: '1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 96 hours after having become aware of it, notify the personal data breach via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555 to the supervisory authority	Keep the Commission proposal. Article 5 must reaffirm the risk-based nature of the Regulation and its balance of data protection and innovation in the economy, with a corresponding reflection in Article 24. Art 33 is a concrete example of overregulation caused by being non-risk based. Businesses are reporting low-risk breaches such as wrongly sent e-mails that supervisory authorities are forced to

	competent in accordance with Article 55 and Article 56. Where the notification to the supervisory authority is not made within *96* hours, it shall be accompanied by reasons for the delay.'	supervisory authority competent in accordance with Article 55 and Article 56 **of this Regulation**. Where the notification to the supervisory authority is not made within ~~96~~ **72** hours, it shall be accompanied by reasons for the delay.'	competent in accordance with Article 55 and Article 56. Where the notification to the supervisory authority is not made within 96 hours, it shall be accompanied by reasons for the delay.'	spend time evaluating, thus worsening data protection. It is vital that the Commission suggestion to only report high risk breaches is passed. The extra added time is good for businesses to ensure proper documentation is gathered before reporting the breach. Furthermore streamlining those reporting requirements is crucial. Businesses often become subject to several reporting mechanisms for security incidents under NIS2, CRA, GDPR, and DORA, creating undesirable overlap and double work.
Article 3, paragraph 9 (amending GDPR Article 35)	Article 35 is amended as follows: (a) paragraphs 4, 5 and 6 are replaced by the following: 4. The Board shall prepare and transmit to the Commission a proposal for a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. 5. The Board shall prepare and transmit to the Commission a proposal for a list of the kind of processing operations for which no data protection impact assessment is required. 6. The Board shall prepare and transmit to the Commission a proposal for a common template and a common	Article 35 is amended as follows: (a) paragraphs 4, 5 and 6 are replaced by the following: '4. The Board shall ~~prepare and transmit to the Commission a proposal for~~ ***establish and make public*** a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. 5. The Board shall ~~prepare and transmit to the Commission a proposal for~~ ***establish and make public*** a list of the kind of processing operations for which no data protection impact assessment is required.	Article 35 is amended as follows: (a) paragraphs 4, 5 and 6 are replaced by the following: 4. The Board shall prepare and transmit to the Commission a proposal for a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. 5. The Board shall prepare and transmit to the Commission a proposal for a list of the kind of processing operations for which no data protection impact assessment is required. 6. The Board shall prepare and transmit to the Commission a proposal for a common template and a common	We further propose that Article 35(9), regarding the requirement to involve the data subject, be removed: ~~9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.~~

	methodology for conducting data protection impact assessments.' (b) the following paragraphs are inserted: '6a. The proposals for the lists referred to in paragraphs 4 and 5 and for the template and methodology referred to in paragraph 6 shall be submitted to the Commission within [OP date = 9 months of the entry into application of this Regulation]. The Commission after due consideration reviews them, as necessary, and is empowered to adopt them by way of an implementing act in accordance with the examination procedure set out in Article 93(2). 6b. The lists and the template and methodology referred to in paragraph 6a- shall be reviewed at least every three years and updated where necessary. The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6a. 6c. Lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data	6. The Board shall ~~prepare and transmit to the Commission a proposal for~~ ***establish and make public*** a common template and a common methodology for conducting data protection impact assessments.' (b) the following ~~paragraphs are~~ ***paragraph is*** inserted: '6a. The proposals for the lists referred to in paragraphs 4 and 5 and for the template and methodology referred to in paragraph 6 shall be ~~submitted to the Commission~~ ***published*** within [OP date = 9 months of the entry into application of this Regulation]. The Commission ~~after due consideration reviews them, as necessary, and is empowered to~~ ***may adopt them the template as established by the Board*** by way of an implementing act, in accordance with the examination procedure set out in Article 93(2). 6b. The lists and the template and methodology referred to in paragraph 6a- shall be reviewed ***by the Board*** at least every three years and updated where necessary. The ~~Board shall submit its assessment and possible proposals for updates to the~~ Commission ~~in due time. The Commission after due consideration of the proposals reviews them and is empowered to~~ ***may*** adopt any updates	methodology for conducting data protection impact assessments.' (b) the following paragraphs are inserted: '6a. The proposals for the lists referred to in paragraphs 4 and 5 and for the template and methodology referred to in paragraph 6 shall be submitted to the Commission within [OP date = 9 months of the entry into application of this Regulation]. The Commission after due consideration reviews them, as necessary, and is empowered to adopt them by way of an implementing act in accordance with the examination procedure set out in Article 93(2). 6b. The lists and the template and methodology referred to in paragraph 6a- shall be reviewed at least every three years and updated where necessary. The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6a. 6c. Lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data	

	protection impact assessment is required established and made public by supervisory authorities remain valid until the Commission adopts the implementing act referred to in paragraph 6a.'	***of the template by way of an implementing act*** following the procedure ***referred to*** in paragraph 6a. 6c. Lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data protection impact assessment is required established and made public by supervisory authorities remain valid until the ~~Commission adopts the implementing act~~ ***Board establishes and makes public the lists*** referred to in paragraph ~~6a~~ ***4 and 5***.'	protection impact assessment is required established and made public by supervisory authorities remain valid until the Commission adopts the implementing act referred to in paragraph 6a.'	
Article 3, paragraph 10 (introducing new GDPR article 41a)	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; (b) develop criteria and or categories for controllers and recipients to assess the risk of re-identification in relation to typical recipients of data.	10.The following article is added: 'Article ~~41a~~**29a - Application of pseudonymisation and identification of a natural person** (1) ~~The Commission may adopt implementing acts to specify means and criteria to determine whether data resulting from~~ **Controllers and processors may apply** pseudonymisation ~~no longer constitutes~~ **to** personal data ~~for certain entities~~ **in order to reduce the risks to the data subjects concerned and to help meet their obligations under this Regulation.** **1a. To determine whether a natural person is identifiable, account shall be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another**	10.The following article is added: 'Article 41a (1) The Commission may adopt implementing acts to specify means and criteria to determine whe**n**~~ther~~ data ~~resulting from pseudonymisation no longer constitutes personal data for certain entities.~~ **a) is merely transitory in nature** **b) is unrelated to the data subject as an identified or identifiable natural person** **c) has appropriate technical and/or organisational safeguards to prevent any use for a purpose related to the data subject as an identified or identifiable natural person**	The Nordic Business Federations support the use of delegated acts to codify requirements of GDPR instead of soft law in EDPB guidance, which is based on compromises between the national authorities in member states and too often have an overly broad focus on rights of the data subjects, instead of a right that should be considered in relation to its function in society and balanced against other fundamental rights, in accordance with the principle of proportionality. Thus, we encourage that the Commission play a larger role in interpreting the GDPR consistent with its intended purpose.

	(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).'	**person to identify the natural person directly or indirectly.** (2) ~~For the purpose of paragraph 1 the Commission~~ **The Board** shall: **issue an opinion, in accordance with Article 64(2) of this Regulation, addressing the application of pseudonymisation and anonymisation, including related technical and organisational measures, and specifying means and criteria to determine whether and when the application of pseudonymisation to personal data may effectively prevent persons other than the controller from identifying a data subject, in such a way that, for them, the data subject is not or is no longer identifiable.** ~~(a) assess the state of the art of available techniques;~~ ~~(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~~ **Chair** 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~~ **Board shall request the opinion referred to in paragraph 1 no later than 12 months after the entry into force of this Regulation. The opinion shall be reviewed and updated where necessary.**	(2) For the purpose of paragraph 1 the Commission shall: (a) assess the state of the art of available techniques; (b) develop criteria and or categories for controllers and recipients to assess the risk of ~~re-identification in relation to typical recipients of data.~~ **data being used for a purpose related to the data subject as an identified or identifiable natural person** (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~~ **be used for any purpose related to the** data subjects **as an identified or identifiable natural person.** (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.	

		~~(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).~~		
Article 3, paragraph 12(a), 13 and 14 (amending GDPR article 70)	13. In Article 70(1), point (h) is deleted. 14. In Article 70(1), the following points are inserted: '(ha) prepare and transmit to the Commission a proposal for a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment and for which no data protection impact assessment is required, pursuant to Article 35. (hb) prepare and transmit to the Commission a proposal for a common template and a common methodology for conducting data protection impact assessments, pursuant to Article 35. (hc) prepare and transmit to the Commission a proposal for a common template for notifying a personal data breach to the competent supervisory authority as well as for a list of the circumstances in which a personal data breach is likely to result in a high risk to	12a. **In Article 70(1), point (f) is amended as follows:** **(f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(1);** 13. In Article 70(1), point (h) is deleted. 14. In Article 70(1), the following points are inserted: '(ha) ~~prepare and transmit to the Commission a proposal for~~ **establish** a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment and for which no data protection impact assessment is required, pursuant to Article 35. (hb) ~~prepare and transmit to the Commission a proposal for~~ **establish** a	13. In Article 70(1), point (h) is deleted. 14. In Article 70(1), the following points are inserted: '(ha) prepare and transmit to the Commission a proposal for a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment and for which no data protection impact assessment is required, pursuant to Article 35. (hb) prepare and transmit to the Commission a proposal for a common template and a common methodology for conducting data protection impact assessments, pursuant to Article 35. (hc) prepare and transmit to the Commission a proposal for a common template for notifying a personal data breach to the competent supervisory authority as well as for a list of the circumstances in which a personal data breach is likely to result in a high risk to	The Nordic Business Federations support the use of delegated acts to codify requirements of GDPR instead of soft law in EDPB guidance. EDPB soft law is based on compromises between the national authorities in member states and too often have an overly broad focus on rights of the data subjects, instead of a right that should be considered in relation to its function in society and balanced against other fundamental rights, in accordance with the principle of proportionality. Thus, we encourage that the Commission play a larger role in interpreting the GDPR consistent with its intended purpose. We therefore we strongly support keeping the EU Commissions proposal and Article. However, we do agree with the Council that a list of circumstances where a breach is not likely to result in a

	the rights and freedoms of a natural person pursuant to Article 33'	common template and a common methodology for conducting data protection impact assessments, pursuant to Article 35. (hc) ~~prepare and transmit to the Commission a proposal for~~ **establish** a common template for notifying a personal data breach to the competent supervisory authority as well as for a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person pursuant to Article 33 **and a list of the circumstances in which it is not likely to result in a high risk.** **(hca) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the appropriate technical and organisational measures to ensure a level of security appropriate to the level of risk pursuant to Article 32.** **(hcb) issue the opinion on the application of pseudonymisation and anonymization referred to in Article 29a.'**	the rights and freedoms of a natural person pursuant to Article 33 **and a list of the circumstances in which it is not likely to result in a high risk.'**	high risk, will reduce uncertainty and be beneficial for companies to help them assess whether to report a breach (and notify individuals, which to our understanding will have the same benchmark for the obligation to apply). Furthermore, we support guidelines specifying appropriate technical and organisational measures in accordance with article 32. Such guidelines are important to keep within the risk-based nature of the regulation, ensuring that companies are still able to choose between a variety of technical and organisational measures and accept proper residual risk in accordance with the specific data controllers risk profile. Those guidelines can be issued in accordance with the current framework thus we do not propose to have them amended in accordance with the Council proposal.
Article 3, paragraph 15 (introducing new GDPR article 88a)	15.After Article 88, the following articles are added: 'Article 88a Processing of personal data in the terminal equipment of natural persons 9547/26 38 GIP.B LIMITE EN (1) Storing of personal data, or gaining of	15.After Article 88, the following articles are added: ~~'Article 88a Processing of personal data in the terminal equipment of natural persons 9547/26 38 GIP.B LIMITE EN (1) Storing of personal data, or gaining of~~	Keep if 88b is deleted	Article 88a (Commission Proposal) should be retained, as it provides a proportionate and effective means to reduce consent fatigue by expanding the whitelist for low-risk, strictly necessary purposes. This will directly and

	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 communications 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 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	~~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 communications 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 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~~		significantly decrease the volume of consent requests for users. Special consideration should be given to statistics on the usage of an online service and security, as those alleviate practical business needs.

	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; 9547/26 39 GIP.B LIMITE EN (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]	~~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; 9547/26 39 GIP.B LIMITE EN (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]~~		
Article 3, paragraph 15 (introducing new GDPR article 88b)	Article 88b Automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons (1) Controllers shall ensure that their online interfaces allow data subjects to: (a) Give consent through automated and machine-readable means, provided that	Article ~~88b~~ 8a **Consent through** automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons (1) **For the purpose of data subject consent to the storing of personal data, or gaining of access to personal data already stored in the terminal equipment of a natural person in**	Delete	Article 88b and 8a should be withdrawn. It introduces far-reaching structural changes that are neither necessary nor sufficiently assessed. The proposal risks reinforcing market concentration, increasing dependencies on dominant gatekeepers, and raises serious concerns regarding compliance with GDPR consent requirements.

	the conditions for consent laid down in this Regulation are fulfilled; (b) decline a request for consent and exercise the right to object pursuant to Article 21(2) through automated and machine-readable means. (2) Controllers shall respect the choices made by data subjects in accordance with paragraph 1. (3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service. (4) The Commission shall, in accordance with Article 10(1) of Regulation (EU) 1025/2012, request one or more European standardisation organisations to draft standards for the interpretation of machine-readable indications of data subjects' choices. Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 1. (5) Paragraphs 1 and 2 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation]. (6) Providers of web browsers, which are not SMEs, shall provide the technical	**accordance with Directive 2002/58/EC**, controllers shall ensure that their online interfaces allow data subjects to: (a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled; (b) ~~decline~~**refuse** a request for consent ~~and~~**or** exercise the right to object pursuant to Article 21(2) through automated and machine-readable means; **(ba) withdraw consent through automated and machine-readable means.** (2) Controllers shall respect **automated and machine-readable means expressing** the choices made by data subjects in accordance with paragraph 1. (3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service. (4) The Commission shall, ~~in accordance with Article 10(1) of Regulation (EU) 1025/2012~~, request one or more European standardisation organisations to draft standards for the interpretation of machine-readable indications of data		In light of the above comments on 88a+b, the priority should be to adopt 88a as a targeted simplification measure, while discontinuing work on 88b and instead pursuing a more evidence-based and future-proof approach, including the development of privacy-enhancing technologies

	means to allow data subjects to give their consent and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to 5 of this Article. Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation].	subjects' choices, **subject to consultation, in accordance with Article 10 of Regulation (EU) 1025/2012**. Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 1. (5) Paragraphs 1 and 2 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation]. (6) Providers of web browsers, ~~which are not SMEs~~, **and providers of operating systems of terminal equipment in relation to software applications operating on that terminal equipment** shall provide the technical means to allow data subjects to give their consent, **to withdraw consent**, and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to ~~5~~4 of this Article.		

		(7) Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation]. **7a. Providers of web browsers and providers of operating systems of terminal equipment in relation to software applications operating on that terminal equipment shall not process the data subject's choices referred to in paragraph 1 for any other purpose than transmitting the signal to providers of online interfaces.**		
Article 3, paragraph 15 (introducing new GDPR article 88c)	Article 88c Processing in the context of the development and operation of AI. Where the processing of personal data is necessary for the interests of the controller 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, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a	~~Article 88c~~ ~~Processing in the context of the development and operation of AI Where the processing of personal data is necessary for the interests of the controller 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, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a~~	Article 88c Processing in the context of the development and operation of AI. Where the processing of personal data is necessary for the interests of the controller 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, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a	A very important proposal to improve competitiveness and AI-development. Keep the Commission's proposal. Processing of special category data (SCD) for developing technology, AI systems and models is currently highly challenging. For large-scale datasets, consent is not a viable legal basis, and alternative bases are rarely available. As AI models—particularly large language models—are trained on vast datasets, often including scraped internet content, it is in practice nearly impossible for commercial actors to process SCD, even where data is highly de-identified. Restrictions on SCD processing should apply only where the purpose is to reveal such data, and "revealing" should not

	child. Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.'	~~child. 9547/26 41 GIP.B LIMITE EN Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.'~~	child. Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.'	include any purely theoretical possibility of identifying sensitive traits. A new legal basis should be introduced for processing de-identified or non-personal uses of SCD. Alternatively, a stricter legitimate interest test tailored to SCD could be developed.
Article 6, paragraph 1, (introducing new NIS 2 article 23a)	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.	1. The following Article 23a is added: 'Article 23a ~~Single-entry point for~~ Incident reporting ***information point*** (1) ENISA shall develop and maintain a ~~single-entry~~ ***an incident reporting information 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~~ ***incident reporting information 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 **National** single-entry point**s and interoperability for incident reporting/data breaches** **(1) Member States shall ensure the establishment of a national single-entry point for the notification of incidents under Union legal acts providing for such obligations.** **(2) ENISA shall make a definition of what constitutes a significant incident that should be reported to the national single-entry point.**	Businesses in the EU are subject to several reporting mechanisms for security incidents under NIS2, CRA, GDPR, and DORA, creating undesirable overlap and double work. For example, different bumpers exist for security incidents in the CRA, DORA and NIS2, and different reports are required for the same event due to diverging requirements in the various acts. The reporting deadlines are also inconsistent. Uploading to the reporting platform is merely the final step in a longer process. To achieve an actual reduction in administrative burdens for European businesses it is necessary to harmonise all steps within the security incident reporting process. Work towards greater alignment of reporting

	(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: (a) the necessary capability for interoperability with regard to other relevant reporting obligations referred to in paragraph (1) is ensured;	~~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.~~ ***2a. The incident reporting information point shall:*** ***(a) enable the identification of applicable obligations to report incidents and related events referred to in paragraph 1;*** ***(b) be designed to allow, on the basis of relevant information provided, to identify the applicable reporting obligations and to be redirected to the appropriate national entry point referred in Article 23b;***	(3) ENISA shall develop and maintain a ~~single-entry~~ ***an incident reporting information*** *point* to support the obligation to report incidents and related events under the Union legal acts where those Union legal acts provide so. **(4) Entities shall submit incident notifications within 96 hours to the national single-entry point of their Member State of main establishment.** **(5) The competent authorities, including CSIRTs, shall process the notifications and, where required under Union law, transmit relevant information to ENISA. Entities shall not be required to report directly to ENISA.** **(6) Member States shall ensure interoperability between national single-entry points, including secure and automated transmission of information where cross-border notifications are required.** **(7) ENISA shall support interoperability and convergence by developing common technical standards and promoting a harmonised reporting template aligned with international standards.**	requirements, including timelines (96 hours) and trigger points, to reduce unnecessary administrative burden and duplication. Deliver a European harmonized secure interoperable technical infrastructure to connect national established Single-Entry Points (SEPs) for reporting that facilitates entities in scope of multiple legal incident reporting obligations to submit one report to be compliant with all applicable rules. See example of Luxembourg and Denmark. We support the settingup of one integrated reporting portal per Member State, covering all statutory reporting obligations, coupled with full EU interoperability through uniform technical and functional standards; and automated and secure transmission where crossborder notifications are required. Companies in all sectors should be allowed to leverage their country of main establishment as the primary interface (single entry point) for cybersecurity incident reporting under relevant EU legislation, provided that this is combined with common templates, definitions and deadlines, and with automated, secure transmission to competent authorities in Member States via national single entry points where cross border notifications are required. ENISA's role should be

	(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	***(c) make available simplified and documented information on incident notification processes in the different Member States, such as help guides or tutorials.*** ***2b. When developing the incident reporting information point, ENISA shall consultthe relevant national competent authorities under the relevant Union legal acts, the NIS Cooperation Group and the CSIRT Network. ENISA shall establish structured communication channels ensuring that information available on the single-information point is swiftly and effectively updated. Member States shall communicate to ENISA all relevant and necessary information for the purpose of paragraph 2a.*** ***2c. The incident reporting information point shall not enable the submission, transmission, storage or processing of any incident notification or related data, and shall not collect any information allowing the identification of the notifying entity or of any incident.*** ***2d. After establishing the incident reporting information point and in cooperation with the NIS Cooperation Group, ENISA shall explore the possibility to extend the incident***		supportive and focus on standardisation, interoperability and quality assurance.

	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	***reporting information point by providing a report on:*** ***(a) regulatory mapping of relevant EU legal acts imposing cybersecurity risk management measures;*** ***(b) national measures, including transposition measures, implementing relevant Union legal acts imposing cybersecurity risk management obligations;*** ***(c) content to support entities in complying with obligations, in particular regarding entity registration, and cybersecurity risk-management.*** ~~(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;~~		

	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, 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.'	~~(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 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, 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.~~		