Council of the European Union

Brussels, 21 May 2026
(OR. en)

9547/26

Interinstitutional File:
2025/0360 (COD)

LIMITE

SIMPL 108
ANTICI 111
DATAPROTECT 167
CYBER 241
TELECOM 254
CODEC 974
PROCIV 106
COMPET 597
MI 511

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Digital Omnibus - Presidency compromise text (GDPR, e-privacy, cookies, P2B, cyber provisions)

Delegations will find attached the Presidency revised compromise text on the Digital Omnibus (GDPR, e-privacy, cookies, P2B, cyber provisions) in view of the AGS meeting of 27 May 2026.

2025/0360 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[1],

Having regard to the opinion of the European Central Bank[2],

Having regard to the opinion of the Committee of the Regions[3],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) In its Communication on a simpler and faster Europe[4] , the Commission announced its commitment to an ambitious programme to promote forward-looking, innovative policies

---

1 OJ C […], […], p. […].
2 OJ C […], […], p. […].
3 OJ C […], […], p. […].
4 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A simpler

that strengthen the Union's competitiveness and radically lighten the regulatory load for people, businesses and administrations, while maintaining the highest standard in promoting the Union's values. Consequently, the Commission prioritised the proposal of immediate adjustments to legislation, including digital legislation, to address the competitiveness challenge of the Union.

(2) Union digital legislation sets high standard in the Union and can be a powerful source of competitive advantage for businesses that abide by the rules, showing a world-leading mark of quality, safety and trustworthiness. Digital regulations have framed the clear rules of the game in the Union for responsible businesses, ensuring fairness and transparency in business-to-business relations, stimulating innovative business models, setting high standard of consumer protection and safety, and for the protection fundamental rights, not least privacy and data protection.

(3) Union digital legislation has evolved incrementally over the past years, in response to the rapidly growing footprint of digital technologies in the Union's economy and societal dynamic, and in view of addressing emerging challenges and promoting business opportunities in the EU. Notwithstanding the Commission's commitment to a systematic 'stress test' of the digital rules, along with other Union rules, which might lead to further regulatory adjustments notably following the forthcoming Digital Fitness Check, as well as other targeted evaluations of digital rules, immediate regulatory changes are necessary. Consequently, this Regulation proposes a first set of amendments to the digital legislative framework, aimed at providing immediate regulatory clarifications that stimulate innovation in the Union market, and that cut administrative compliance costs in particular for businesses, while also streamlining supervisory and administrative costs for supervisory authorities and advisory bodies. The amendments also seek to provide clarity to individuals.

(…)

(27) This Regulation proposes a series of targeted amendments to Regulation (EU) 2016/679 for clarification and simplification, whilst preserving the same level of data protection. ~~Article 4 of Regulation (EU) 2016/679 provides that personal data is any information~~

---

and faster Europe: Communication on implementation and simplification, COM(2025)47 final, 11 February 2025

~~relating to an identified or identifiable natural person. In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. Taking into account the case-law of the Court of Justice of the European Union concerning the definition of personal data, it is necessary to provide further clarity on when a natural person should be considered to be identifiable. The existence of additional information enabling the data subject to be identified does not, in itself, mean that pseudonymised data must be regarded as constituting, in all cases and for every person or entity, personal data for the purposes of the application of Regulation (EU) 2016/679. In particular, it should be clarified that information is not to be considered personal data for a given entity where that entity does not have means reasonably likely to be used to identify the natural person to whom the information relates. A potential subsequent transmission of that information to third parties who have means reasonably allowing them to identify the natural person to whom the information relates, such as cross-checking with other data at their disposal, renders that information personal data only for those third parties who have such means at their disposal. An entity for which the information is not personal data, in principle, does not fall within the scope of application of Regulation (EU) 2016/679. In this respect the Court of Justice of the European Union has held that a means of identifying the data subject is not reasonably likely to be used where the risk of identification appears in reality to be insignificant, in that the identification of that data subject is prohibited by law or impossible in practice, for example because it would involve a disproportionate effort in terms of time, cost and labour. An example of a prohibition against reidentification can be found in the obligations of health data users in Article 61(3) of Regulation (EU) 2025/327 of the European Parliament and of the Council[5]. The Commission, together with the European Data Protection Board, should support controllers in the application of this updated definition by stipulating technical criteria in an implementing act.~~

(27a) In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. The identification of a natural person should be assessed by the

---

[5] ~~Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (OJ L, 2025/327, 5.3.2025, ELI: http://data.europa.eu/eli/reg/2025/327/oj)~~

controller or the processor, considering the actual technical, organisational and legal capabilities of the controller or processor. In light of the interpretation provided in the case-law of the Court of Justice of the European Union, it is important to provide further clarity on when a natural person should be considered to be identifiable following the application of pseudonymisation to personal data and the transmission to a recipient. The European Data Protection Board should ensure consistency and support controllers by adopting an opinion on pseudonymisation and anonymisation, assessing and specifying the state of the art of available techniques, as well as the technical and organisational measures and criteria to apply pseudonymisation and anonymisation to personal data effectively and by clarifying circumstances whether and when the application of pseudonymisation to personal data may effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable. The opinion should also address the processing to be undertaken and other measures to be applied in order to effectively render personal data anonymous. It is important that the Board carries out a public consultation with relevant stakeholders prior to issuing its opinion. While controllers remain fully responsible to determine and demonstrate whether pseudonymised data do not lead to re-identification of data subjects by persons other than the controller, the opinion should support and provide guidance to controllers regarding the effective application of pseudonymisation to personal data.

(27b) **Pseudonymisation is one of the possible security measures within the meaning of Article 32 of Regulation (EU) 2016/679 and does not necessarily have to be applied in all cases. Whether pseudonymisation is appropriate, should be assessed on a case-by-case basis and depends on the context, the nature of the personal data and the existence of other appropriate technical and organisational measures. The effective application of pseudonymisation may also be clarified for controllers and processors through the approval of specific codes of conduct in accordance with Article 40 of Regulation (EU) 2016/679, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises.**

(28) In order to assess whether **scientific** research ~~meets~~ **activities meet** the conditions of scientific research for the purpose of ~~this~~ Regulation **(EU) 2016/679**, account can be taken of elements such as **the purpose of the research, the** methodological ~~and systematic~~

approach **and ethical standards** applied **in the specific area** while conducting the research**, and adherence to the principles of transparency, reliability, accountability, oversight, verifiability, and rules for research integrity** ~~in the specific area~~. **Transparency may, among other things, involve making research results publicly available with due regard to legitimate limitations to access such as protection of intellectual property and trade secrets. Scientific research activities should be conducted autonomously and independently, free from undue pressure and contribute to the growth of society's general knowledge and wellbeing. This does not exclude that the outcome of scientific research activities may also aim to further commercial or private interests.**

It is important that processing for scientific research activities prevent individuals from being subjected to harm or other adverse effects due to their participation in scientific research and **respect, amongst others, human autonomy and, to the extent necessary, the notion of consent to participate in research should be used as a safeguard and is to be considered distinctively from consent under Regulation (EU) 2016/679. Scientific research can, amongst others, be part of and support innovation, such as** technology **or medical** development**. Scientific research activities may** ~~should~~ be conducted in academic, industry and other settings, **by public authorities or private entities,** including small and ~~medium-sized~~**medium sized** undertakings**. The outcome of scientific research may be applied for public interest, private or commercial purposes.**

The qualification of processing as being carried out for scientific research purposes~~,~~ ~~(Article 179(2) TFEU) and~~ should be ~~always of a of high quality~~**assessed on a case-by-case basis, considering the objective characteristics of the research activity,** and should ~~adhere to the principles of principles of reliability, honesty, respect and accountability (verifiability~~**not rely solely on the declaration of the controller, nor undermine the obligation to apply appropriate safeguards as provided for in Article 89 of Regulation (EU) 2016/679**.

(29) It should be reiterated that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. In such cases it ~~is not~~**should not be** necessary to ascertain on the basis of Article 6(4) of ~~this~~ Regulation **(EU) 2016/679** whether the purpose of the further processing is compatible with the purpose for which the personal data are initially collected. **Such further processing should be considered compatible,**

provided that it is carried out in compliance with the principles and appropriate safeguards laid down in Regulation (EU) 2016/679, in particular Article 89.

~~(30) Trustworthy AI is key in providing for economic growth and supporting innovation with socially beneficial outcomes. The development and use of AI systems and the underlying models such as large language models and generative video models rely on data, including personal data, in various phases in the AI lifecycle, such as the training, testing and validation phase and may in some instances be retained in the AI system or the AI model. The processing of personal data in this context may therefore be carried out for purposes of a legitimate interest within the meaning of Article 6 of Regulation (EU) 2016/679, where appropriate. This does not affect the obligation of the controller to ensure that the development or use (deployment) of AI in a specific context or for specific purposes complies with other Union or national law, or to ensure compliance where its use is explicitly prohibited by law. It also does not affect its obligation to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.~~

~~(31) 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, 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.~~

(32) The processing of personal data for scientific research purposes and the application of the GDPR's provisions on scientific research are conditional on the adoption of appropriate safeguards for the rights and freedoms of data subjects, pursuant to Article 89(1) GDPR. To that end, the GDPR balances the right to protection of personal data, pursuant to Article 8 CFREU, with the freedom of science, pursuant to Article 13 CFREU. The processing of personal data for the purpose of scientific research ~~therefore pursues a~~**can follow public interest within the meaning of Article 6(1)(e) of Regulation (EU) 2016/679 or be based on Member States and Union law. The processing of personal data for the purpose of scientific research may also be necessary for the purposes of the** legitimate ~~interest~~**interests pursued by a controller or by a third party** within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, provided that such research is not contrary to Union or Member State law. This is without prejudice to the obligation of the controller to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.

(33) The development of certain AI systems and AI models may involve the collection of large amounts of data, including personal data and special categories thereof. Special categories of personal data may **incidentally and** residually exist in the training, testing or validation data sets or be retained in the AI system or the AI model, although the special categories of personal data are not necessary for the purpose of the processing **and while the controller did not initially envisage the processing of such personal data and has taken the appropriate technical and organisational measures to avoid such processing**. In order not to disproportionately hinder the development and operation of AI and taking into account the capabilities of the controller to identify and ~~remove~~**erase** special categories of personal data, derogating from the prohibition on processing special categories of personal data under Article 9(2) of Regulation (EU) 2016/679 should be allowed **for incidental and residual processing of special categories of data in the context of the development and operation of AI systems or AI models. The derogation should not be understood as covering the processing of special categories of personal data collected through prompts during the deployment of the AI system or AI models**. The derogation should only apply where the controller has implemented appropriate technical and organisational measures in an effective manner to avoid the processing of those data, takes the appropriate measures during the entire lifecycle**, that is to say during the development and operation,** of an AI system or AI model and, once it identifies such data, effectively ~~remove them. If removal~~**erase them. If erasure** would **prove impossible or** require

manifestly disproportionate effort, notably where the ~~removal~~ erasure of special categories of data memorised in the AI system or AI model would require re-engineering the AI system or AI model, **or would be technically impossible,** the controller should effectively protect such data from **being further processed or processed for other purposes, in particular** being used to infer outputs, being disclosed or otherwise made available to third parties**. In line with the accountability principle, the controller should document its assessment and have processes in place to monitor and demonstrate the effectiveness of these measures**. This derogation should not apply where the processing of special categories of personal data is necessary for the purpose of the processing. In this case, the controller should rely on the derogations pursuant to Article 9(2)(a) – (j) of Regulation (EU) 2016/679 **or on other Union law, such as Regulation (EU) 2024/1689 regarding the processing of special categories of personal data for the purpose of ensuring bias detection and correction**. **The notion of AI system and AI model should be understood in the same manner as in Regulation (EU) 2024/1689.**

(33a) The processing of personal data in the context of the development and deployment of an AI system or of an AI model, may be regarded as carried out for a legitimate interest of the controller concerned and be carried out in accordance with Article 6(1)(f) of Regulation 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 child. This does not affect the obligation of the controller to choose the most appropriate lawful ground of processing set out in Article 6 of Regulation (EU) 2016/679, such as Article 6(1)(e) with regard to processing by public authorities. 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.

(34) **Processing of** biometric data, as defined in Article 4(14) of Regulation (EU) 2016/679, means processing of certain characteristics of a natural person through a specific technical means and which allows or confirms the unique identification of that person. The notion of biometric ~~data~~**recognition** includes two distinct functions, namely the identification of a

natural person or the verification (also called 'authentication') of his or her claimed identity, both of which rely on different technical processes. The identification process is based on a 'one-to-many' search of the data subject's biometric data in a database, while the verification process is based on a 'one-to-one' comparison of biometric data provided by the data subject, who is thereby claiming his or her identity. Derogating from the prohibition to process biometric data under Article 9(1) of ~~the~~ Regulation **(EU) 2016/679** should ~~also~~ be allowed where the verification of the claimed identity of the data subject is necessary for a purpose pursued by the controller~~,~~ and**, where applicable, subject to appropriate safeguards laid down under Union law or Member States law in accordance with Article 9(4) of Regulation (EU) 2016/679. Where biometric data are processed for the purpose of confirming the identity of a data subject, controllers should, where possible, prioritise authentication methods that do not involve the processing of biometric data. The controller should choose from equally effective means the less intrusive one. The processing of biometric data for identity verification should therefore only be used where necessary and proportionate and subject to appropriate safeguards. For the purposes of this Regulation, biometric identification should be understood as the processing of biometric data through comparison against a database intended to determine the identity of a natural person, whereas biometric verification refers to a one-to-one comparison used solely to confirm a claimed identity. This derogation should apply where** suitable safeguards apply to ~~enable the data subject to have~~**ensure that the biometric data or the means needed for the verification are under the** sole control of the **data subject. Sole control means that the data subject can effectively decide when and how his or her biometric data are used for** verification**, without the controller having the technical capacity to access such biometric data in decrypted form or** process **them outside the strictly limited comparison process necessary for verification**. For example, **this is the case** where the biometric data are securely stored solely at the ~~side~~**device** of the data subject or are securely stored ~~at the side of~~**by** the controller in a state-of-the-art encrypted form and the encryption key or equivalent means is **securely** held solely by the data subject, ~~that~~**and subject to measures ensuring the overall security of** processing ~~is not likely to create significant risks to his or her fundamental rights and freedoms. The controller does not gain knowledge of the~~**, including during the enrolment phase of data subject's** biometric data ~~or only for a very limited time~~**and** during the verification process. **Such verification may in particular be required in the context of electronic identification**

systems and trust services under Union law. Other examples of appropriate safeguards are ensuring that end-to-end encryption is used when data are transmitted over a communication channel and providing data subjects with the possibility to securely erase their biometric data at any time.

(35) **Chapter III of Regulation (EU) 2016/679 sets out rights of the data subject and corresponding obligations of the controller. Inter alia,** Article 15 of Regulation (EU) 2016/679 provides data subjects with the right to obtain **confirmation** from the controller ~~confirmation~~ as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and certain additional information. The right of access should allow the data subject to be aware of, and to verify, the lawfulness of the processing and enable him or her to exercise his or her other rights under Regulation (EU) 2016/679. ~~By contrast, it should be clarified in~~ Article 12 **(5) of that**~~of the~~ Regulation **already provides that where the request to exercise a**~~that the~~ right ~~of access, which is from the outset favourable to data subjects,~~**under Regulation 2016/679 is manifestly unfounded or excessive, the controller may either charge a reasonable fee or refuse to act on the request. The controller** should ~~not be abused in the sense that~~**provide** the data ~~subjects abuse them for purposes other than the protection of their data~~**subject with the reason thereof. A request is also to be considered excessive where an abusive intention on the part of the data subject submitting those requests can be demonstrated by the controller**. For example, such an ~~abuse of the right of access~~**abusive intention** would arise where the data subject ~~intends to cause the controller to refuse an access request, in order to subsequently demand the payment of compensation, potentially under the threat of bringing a claim for damages. Other examples of abuse include situations where data subjects make~~**submits** excessive ~~use of the right of access~~**numbers of identical or largely similar requests** with the ~~only~~**sole** intent of causing damage or harm to the controller ~~or when~~**. Repeated requests are not automatically excessive in nature but may indicate an abusive intent on the part of the data subject. Other examples include situations where** an individual ~~makes~~**submits** a request, but at the same time offers to withdraw it in return for some form of benefit from the controller~~. Moreover, in order to keep their burden to a reasonable extent, controllers should bear a lower burden of proof regarding the excessive character of~~**, when an subject submits** a request ~~than regarding the manifestly unfounded character of a request. The reason is that the manifestly unfounded character of a request depends on facts that lie principally within the controller's sphere of responsibility, whereas the excessive character~~

~~of a request concerns the possibly abusive conduct of a data subject,~~**with the sole purpose of obtaining compensation for an alleged infringement** which ~~lies primarily outside the controller's sphere of influence, and therefore the controller may be able to prove such abuse only to a reasonable level. In any event, while requesting access under Article 15 of Regulation (EU) 2016/679~~**is deliberately provoked by** the data subject ~~should be as specific as possible. Overly broad and undifferentiated requests should also be regarded as excessive~~**, or when the exercise of a right is made with the intention to adversely affect a judicial procedure or with deliberate intention to adversely affect and burden public authorities**.

(35a) Article 57 of Regulation (EU) 2016/679 provides rules for situations where requests from a data subject to the supervisory authority, including complaints under Article 77 of Regulation (EU) 2016/679, are manifestly unfounded or excessive, in particular because of their repetitive character. Articles 12 and 57 of Regulation (EU) 2016/679 use the same wording and pursue the same objective, namely to provide for an exception to the free-of-charge principle applicable to the tasks carried out by the supervisory authorities and the exercise of rights of the data subject, respectively. In order to reduce the burden of controllers with regard to excessive requests, which may also occur in relation to requests, including complaints, to the supervisory authority concerning the controller, the notion of excessiveness in Article 57 of Regulation (EU) 2016/679 should be adapted likewise.

(36) Article 13 of Regulation (EU) 2016/679 requires the ~~data~~ controller to provide the data subject with certain information on the processing of his or her personal data as well as certain further information necessary to ensure fair and transparent processing, as defined in paragraphs 1, 2 and 3 of that provision. According to paragraph 4 of Article 13 of Regulation (EU) 2016/679, that obligation does not apply where and insofar as the data subject already has the information. To further reduce the burden of ~~data~~ controllers, without undermining the possibilities of the data subject to exercise his or her rights under Chapter III of ~~the~~**that** Regulation, this derogation should be extended to situations **where the personal data have been collected in the context of a clear and circumscribed relationship between a data subject and a controller exercising an activity that does not involve processing a large amount of personal data,** where the processing is not likely to result in a high risk, within the meaning of Article 35 of ~~the~~**that** Regulation, and there are reasonable grounds to ~~assume~~**believe** that the data subject already has the

information referred to in points (a) and (c) of paragraph 1 **of Article 13** in the light of the context in which the personal data have been collected~~, in particular regarding the~~**. A clear and circumscribed** relationship ~~between data subjects and the controller. These should be the situations where the context of the relationship between~~**requires** the controller and the data subject ~~is very clear and circumscribed and the controller's activity is not data-intensive,~~**to have a direct relationship** such as the relationship between a craftsman and their clients**. The application of the derogation from the information obligation should not undermine the principle of transparency and should be limited to situations where the controller has reasonable grounds to believe that the data subject already possesses the required information. These should be the situations where the personal data are collected in the context of a direct and clearly circumscribed relationship between data subjects and a controller and does not involve the processing of a large amount of personal data**, **and** where the scope of processing is limited to the minimum data necessary to perform the service. ~~The controller's activity is not data-intensive where it collects a low amount of personal data and its processing operations are not complex, which is not the case, for example, in the field of employment.~~ In such ~~circumstances, that is to say when the processing is non data-intensive, non-complex and where the controller collects a low amount of personal data~~**cases**, it should be reasonable to expect, for instance, that the data subject has the information on the identity and contact details of the controller**,** as well as on the purpose of ~~the~~ processing ~~when that processing is carried out for the performance of a contract to which a data subject is a party, or when the data subject has given his or her consent to that processing, in accordance with the requirements laid down in Regulation (EU) 2016/679~~.- The same should apply**, under the aforementioned conditions,** to associations and sport clubs where the processing of personal data is confined to the management of membership, communication with members and the organisation of activities. Nevertheless, this derogation from the obligations of Article 13 is without prejudice to the independent obligations of the controller under Article 15 of that Regulation, which applies in case the data subject requests access based on the latter provision. **This derogation should only apply to processing operations which are foreseeable and non-complex, which is not the case in the field of employment or in relations with public authorities or public bodies or private entities for the performance of a task in the public interest.** Where the derogation from the obligations of Article 13 does not apply, in order to balance the need for completeness and easy understanding by the data subject,

controllers may adopt a layered approach when providing the information required, notably by allowing users to navigate to further information.

(37) Where the **further** processing **by the same controller** takes place for the purpose of scientific research and the provision of information to the data subject proves to be impossible or would involve a disproportionate effort it should not be necessary to provide the information provided for under Article 13 of this Regulation. The controller should make reasonable efforts to acquire contact details if they are readily available and acquisition would not require a disproportionate effort. The provision of the information would involve a disproportionate effort in particular where the controller at the time of collection of the personal data did not know or anticipate that it would process personal data for scientific research purposes at a later stage, in which case it may not have easily available contact details of the data subjects. In such situations the controller should inform data subjects indirectly, such as by making the information publicly available. The provision of such information should ensure that as many data subjects concerned as possible are reached. Relevant means to make the information publicly available should be determined depending on the context of the research project and the data subjects involved.

(38) Article 22 of Regulation (EU) 2016/679 provides ~~for~~**that data subject has the right not to be subject to a decision based solely on automated processing, except when specific conditions are met and in accordance with** rules governing the processing of personal data when the ~~data~~ controller makes decisions which have legal effects **concerning the data subject** or similarly significant effects on the data subject, based solely on automated processing. In order to provide greater legal certainty, it should be clarified that ~~decisions~~**when assessing whether a decision** based solely on automated processing ~~are allowed when specific conditions are met, as set out in Regulation (EU) 2016/679. It should also be clarified that when assessing whether a decision~~ is necessary for entering into, or performance of, a contract between the data subject and a ~~data~~ controller, as set out in Article 22(2)(a) of Regulation (EU) 2016/679, it should not be required that the decision could be taken only by solely automated processing. ~~This means that~~ The fact that the decision could also be taken by a human does not prevent the controller from taking the decision by solely automated processing**.** When several equally effective automated processing solutions exist, the controller should use the less intrusive one.

(39) ~~In order to reduce the burden on controllers while ensuring that supervisory authorities have access to the relevant information and can act on violations of the Regulation, the threshold for notification of a personal data breach to the supervisory authority under Article 33 of Regulation (EU) 2016/679 should be aligned with that of communication of a personal data breach to the data subject under Article 34 of that Regulation.~~ In the case of a data breach that is not likely to result in a high risk to the rights and freedoms of natural persons, the controller should not be required to notify the competent supervisory authority. The higher threshold for notifying a data breach to the supervisory authority does not affect the obligation of the controller to document the breach in accordance with paragraph 5 of Article 33 of Regulation (EU) 2016/679, or its obligation to be able to demonstrate its compliance with that Regulation, in accordance with Article 5(2) of that Regulation. In order to facilitate compliance by controllers and a harmonised approach in the Union, the Board should ~~prepare~~**establish and make public** a common template for notifying data breaches to the competent supervisory authority and a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person~~. The Commission should take due account of the proposal prepared by the Board and review them, as necessary, prior to adoption~~**, and a common list of circumstances in which a personal data breach does not result in such a high risk**. In order to take account of new information security threats, the common template and the list should be reviewed at least every three years and updated **where necessary. The Commission may adopt, by means of an implementing act, the common template as established by the Board, as well as its updates** where necessary. The lack of a common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person should not affect the obligations of controllers to notify those breaches. **The alignment of notification thresholds should not affect the controller's obligation to carry out an individual risk assessment and to maintain complete documentation of personal data breaches in accordance with Article 33(5) and Article 30 of Regulation (EU) 2016/679. The common list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedom of a natural person should also apply in order to determine when communicating the data breaches to the data subject, in accordance with Article 34.**

(39a) In order to facilitate compliance obligations and the establishment of the contract or other legal act governing the processing by a processor on behalf of the controller, the

processor should also be subject to the general obligation of data protection by design and by default under Regulation (EU) 2016/679 to extent it relates to its own obligations under that Regulation. This obligation on the processor does not affect level of responsibility and relationship between the controller and processor, nor the principle of accountability or the respective obligation of controller and processor as laid down under Article 28 of Regulation (EU) 2016/679). As such, the controller remains solely responsible of determining the purpose and means of processing and apply related obligations, while the processor should ensure that data protection by design and by default is applied to its processing offer and services.

(40) Article 35 of that Regulation (EU) 2016/679 requires controllers to conduct a data protection impact assessment where the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons. The supervisory authorities established pursuant to that Regulation are required to establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. In addition, the Regulation provides that supervisory authorities may establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. In order to effectively contribute to the aim of convergence of the economies and to effectively ensure free flow of personal data between Member States, increase legal certainty, facilitate compliance by controllers and ensure a harmonised interpretation of the notion of a high risk to the rights and freedoms of data subjects, a single list of processing operations should be provided at EU level, to replace the existing national lists. In addition, the publication of a list of the type of processing operations for which no data protection impact assessment is required, which is currently optional, should be made mandatory. The lists of processing operations should be ~~prepared~~**established and made public** by the Board ~~and adopted by the Commission as an implementing act~~**. In establishing the lists, due account should be taken of the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons**. In order to facilitate compliance by controllers, the Board should also ~~prepare~~**establish and make public** a common template and a common methodology for conducting data protection impact assessments~~, to be adopted by the Commission as an implementing act. The Commission should take due account of the proposals prepared by the Board and review them, as necessary, prior to adoption~~. In order to take account of technological developments, the lists and the common template and methodology should be reviewed at least every three years and updated where necessary. **The Commission**

may adopt, by means of an implementing act, the common template as established by the Board, as well as its updates where necessary.

(40a) In order to ensure consistency of interpretation of this Regulation (EU) 2016/679, it is important that national supervisory authorities ensure that the adoption of guidelines, recommendations and best practices at national level on matters already covered by guidelines adopted by the Board, is consistent and does not contradict those issued by the Board, including by updating national relevant guidelines, recommendations and best practices when necessary. It is also important that national supervisory authorities and the Board duly consider matters of consistent application of this Regulation, including when such matters are identified and brought to their attention by controllers or other relevant stakeholders.

(41) Regulation (EU) 2018/1725 of the European Parliament and of the Council[6] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. ~~Directive (EU) 2016/680 of the European Parliament and of the Council[7] applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.~~ Regulation (EU) 2018/1725 ~~and Directive (EU) 2016/680~~ should be brough into alignment with the amendments to Regulation (EU) 2016/679 introduced by this Regulation.

(42) As clarified in recital 5 of Regulation (EU) 2018/1725, whenever the provisions of Regulation (EU) 2018/1725 follow the same principles as the provisions of Regulation (EU) 2016/679, those two sets of provisions should, under the case law of the Court of Justice of the European Union, be interpreted homogeneously. The scheme of Regulation

---

6 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

~~7~~ ~~Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).~~

(EU) 2018/1725 should be understood as equivalent to the scheme of Regulation (EU) 2016/679. Therefore, this Regulation also amends the provisions of Regulation (EU) 2018/1725 that are concerned by the amendments of Regulation (EU) 2016/679, insofar as the latter amendments are also relevant in the context of the processing of personal data by the Union institutions, bodies, offices and agencies.

~~(43) In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Directive (EU) 2016/680 and any other Union legal act applicable to such processing of personal data should follow after the adoption of this regulation, in order to allow for their application as close as possible to the entry into application of the amendments to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.~~

(43a) Directive 2002/58/EC on privacy and electronic communications ('ePrivacy Directive'), last revised in 2009, provides a framework for the protection of the right to privacy, including the confidentiality of communications. It also specifies Regulation (EU) 2016/679 in relation to processing of personal data in the context of electronic communication services. It protects the privacy and the integrity of subscriber's or user's terminal equipment used for such communications.

(44) The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment and the subsequent processing of such data should be regulated under a single legal framework, namely Regulation (EU) 2016/679, where the subscriber of the electronic communications service or the user of the terminal equipment is a natural person. The amendments ~~presented in this Regulation~~**to this Directive should** continue to offer the highest levels of protection for personal data, while simplifying the experiences of data subjects in exerting their rights and expressing their choices online. The amendments concern in particular storage of information in that equipment, accessing or otherwise collecting information from that equipment that entails the processing of personal data through cookies or similar technologies to gain information from the terminal equipment. ~~The relevant rules should also apply regardless of whether the terminal equipment is owned by the natural person or by another legal or natural person.~~

The storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment should continue to be allowed only on the basis of consent. ~~Similar to the approach in Directive 2002/58/EC, this requirement should not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal~~

~~equipment of a natural person, when that is based on Union or Member State law within the meaning of Article 6 of Regulation (EU) 2016/679 and if it fulfils all conditions of lawfulness laid down in that provision, and is done for the objectives laid down in Article 23(1) of Regulation (EU) 2016/679.~~

With a view to reducing the compliance burden and providing legal clarity ~~to controllers~~, and given that certain purposes of processing pose a low risk to the rights and freedoms of data subjects or that such processing may be necessary to provide a service requested by ~~the data subject~~**a subscriber or user**, it is necessary to define a limitative list of purposes for which the processing should be permitted without consent. As regards storing of personal data, or the gaining of access to personal data already stored, in a terminal equipment, and subsequent processing that is necessary for those purposes, ~~this Regulation~~**the Directive** should therefore provide that ~~the~~**such** processing is lawful~~. The~~**, including when being carried out jointly with or on the behalf of a** controller~~, such as~~**. For example,** a media service provider, may mandate a ~~processor~~**third party**, such as a market research company, to carry out **such processing.**

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, or by a processor acting jointly with or on behalf of this provider, also referred to as 'audience measurement', means~~the~~ processing **to obtain insight into the performance and use of the online service in an instantly anonymised, aggregated and general manner. This includes the performance of audience measurement as defined in Regulation (EU) 2024/1083. The aggregated information should not relate to a specific data subject and should therefore be anonymous aggregated information. The data collected should not be further processed for another purpose, combined with data from other services from the provider of the online service or from a third party, such as analytics information from other websites or apps, or shared with third parties.**

Maintaining or restoring the security of a service provided by an information society service provider and requested by the subscriber or user, or the terminal equipment used for the provision of such service, should only be allowed without consent to the extent that the security updates are strictly necessary, proportionate, discretely packaged and do not in any way change the functionality of the software on the terminal equipment, including the interaction with other software or settings chosen by the subscriber or user, the subscriber or user is informed in advance each time an

update is being installed, and the subscriber or user has the possibility to turn off the automatic installation of these updates~~on its behalf~~.

For the ~~subsequent~~**further** processing of personal data for other purpose than those defined in the limitative list, Article 6 and, where relevant, Article 9 of Regulation (EU) 2016/679 should be applied. It is the responsibility of the controller in the light of the principle of accountability to choose the appropriate legal basis for the intended processing. In order to be able to rely on legitimate interest under Article 6(1), point f, of Regulation (EU) 2016/679 as a ground for the ~~subsequent~~**further** processing of personal data, the controller must show that it pursues the controller's or third parties' legitimate interest, the processing is necessary in order to achieve the purpose of that legitimate interest, and the interests or fundamental rights of the data subject do not override the interests pursued by the controller. In this context, controllers should take outmost account of the following elements: whether the data subject is a child; the reasonable expectations of data subject; the impact on the individual either because of the scale of data processed or the sensitivity of the data processed; the scale of the processing at issue in the sense that the processing cannot be particularly extensive either because of their amount or the range of categories of data; the processing should be based on data limited to what is necessary and cannot be based on monitoring of large parts of the online activity of the data subjects; and other relevant factors as appropriate. The processing should not give rise to the continuous monitoring of the data subject's private life.

~~Where the controller cannot rely on legitimate interest as a legal ground for the subsequent processing, the processing should be based on another ground in Article 6(1), in particular on consent in accordance with Articles 6 and 7 of Regulation (EU) 2016/679, provided that all principles of Regulation (EU) 2016/679 are met.~~

(45) Data subjects that have refused a request for consent are often confronted with a new request to give consent each time they visit the same controller's online service again. This may have detrimental effects to the data subjects which may consent just in order to avoid repeating requests. The controller should therefore be obliged to respect the data subject's choices to refuse a request for consent for at least a certain period. **This obligation is applicable to any controller that accesses or stores personal data in the terminal equipment of the data subject, including third party cookie providers.**

(46) Data subjects should have the possibility to rely on automated and machine-readable indications of their choice to consent or refuse a consent request or object to the processing of data. Such means should follow the state of the art. They can be implemented in the settings of a web browser or in the EU Digital Identity Wallet as set out by Regulation (EU) 914/2014, or any other adequate means. Rules set out in this Regulation should support the emergence of market-driven solutions with appropriate interfaces. The controller should be obliged to respect automated and machine-readable indications of data subject's choices once there are available standards. In light of the importance of independent journalism in a democratic society and in order not to undermine the economic basis for that, media service providers should not be obliged to respect the machine-readable indications of data subject's choices. The obligation for providers of web browsers to provide the technical means for data subjects to make choices with respect to the processing should not undermine the possibility for media service providers to request consent by data subjects.

(46a) Standardisation should play a key role to ensure that technical solutions are available for data subjects to easily set their consent preferences and enable them to make granular and informed decisions. In particular, the standards should enable data subjects to consent, refuse consent and exercise the right to object for direct marketing purposes. The standards should ensure that the conditions for consent under Regulation (EU)2016/679 are fulfilled and enable consent for different purposes. The standards should be prepared in a way that takes into account the operation of businesses in a digital environment and that ensures information is promoted in the digital economy and supports access to content and services on the open web. The standards should ensure that consumer law and competition law requirements are appropriately observed, preventing in particular self-preferencing practices in the provision of the technical solutions that enable setting consent choices.

~~(47) Directive 2002/58/EC on privacy and electronic communications 'ePrivacy Directive'), last revised in 2009, provides a framework for the protection of the right to privacy, including the confidentiality of communications. It also specifies Regulation (EU) 2016/679 in relation to processing of personal data in the context of electronic communication services. It protects the privacy and the integrity of user's or subscriber's terminal equipment used for such communications. The current provision of Article 5(3) of~~

~~Directive 2002/58/EC should remain applicable insofar as the subscriber or user is not a natural person, and the information stored or accessed does not constitute or lead to the processing of personal data.~~

(48) Article 4 of Directive 2002/58/EC should be repealed. Article 4 of Directive 2002/58/EC sets requirements for providers of publicly available electronic communications services as regards safeguarding the security of their services and notification requirements. Subsequently, Directive (EU) 2022/2555 has set new requirements as regards cybersecurity risk-management measures and incident reporting for those providers. In order to reduce overlapping obligations for entities in the electronic communications sector, Article 4 of Directive 2002/58/EC should be repealed. As regards the security of processing of personal data pursuant to Article 4(1) and (1a) of this directive and the notification of personal data breaches pursuant to Article 4(3) to (5) of Directive 2002/58/EC this directive, the Regulation (EU) 2016/679 already provide for comprehensive and up-to-date rules. These rules should therefore apply to providers of publicly available electronic communication services and providers of public communications networks, thereby ensuring that one regime applies to the controllers and processors.

(49) Several horizontal or sectorial Union legal acts require the notification of the same event to different authorities using different technical means and channels. The ~~single-entry~~**establishment by Member States of a national entry** point ~~for incident~~ reporting should allow entities to fulfil reporting obligations under Directive (EU) 2022/2555, Regulation (EU) 2016/679, Regulation (EU) 2022/2554, Regulation (EU) No 910/2014 and Directive (EU) 2022/2557 by submitting notifications to a single interface **at national level**. Furthermore, the single-entry point **established at national level** should give a possibility for entities to retrieve information that they have previously submitted using the single-entry point, thereby helping entities to keep track of their compliance with reporting obligations in connection with specific incidents.

(49a) In order to facilitate compliance with the obligation to report incidents and related events, including the identification of the applicable related obligations, ENISA should develop and maintain a single information point for incident reporting. Structured communication channels should be established to ensure that the

information available on the single information point is swiftly updated based on all the relevant and necessary information communicated by Member States.

(50) To ensure the security of ~~the single entry point~~**national entry points in particular and with a view to design interoperable national entry points**, ENISA should ~~take~~**develop guidelines addressing the** appropriate and proportionate technical, operational and organisational measures ~~to manage the risks posed to the security of the single entry~~**for Member States to develop and maintain their respective national entry** point ~~and the information submitted or disseminated via the single entry point. When assessing the risk, and the appropriateness and proportionality of those measures, ENISA should take into account the sensitivity of information submitted or disseminated pursuant to the relevant Union legal acts~~. ENISA should consult competent authorities under the relevant Union legal acts when drafting the technical, operational and organisational measures necessary to establish, maintain and securely operate the ~~single entry~~**national entry** point by making use of existing cooperation groups and networks of Member States established under these acts.

(50a) The term 'national entry point' should be understood as a national infrastructure or arrangement, which may take the form of a digital interface, platform or technical interoperability hub, established and maintained by the Member State, enabling entities to fulfil their incident notification obligations across multiple regulatory frameworks through a single notification at national level which will reach all competent authorities. Member States should retain flexibility to configure such infrastructure or arrangement in accordance with their specific needs, notably their national infrastructures and the allocation of competences among authorities, including by connecting existing systems and enabling the sharing, routing or distribution of relevant information where needed. The creation of the national entry point does not necessarily interfere with the allocation of functions among competent authorities within each national system.

(50b) The development and operation of national entry points may involve important costs for Member States, particularly where national reporting systems need to be built upon existing ones to adapted. It is important that, where applicable and foreseen in the relevant instruments, such activities are financially supported through relevant

Union funding instruments, such as the Digital Europe Programme, the European Structural and Investment Funds and other relevant Union funding programmes.

(51) ~~Before enabling the~~**It is important to support the further harmonisation of incident** notification ~~of incidents, ENISA should pilot the functioning of the single-entry point which should include a thorough testing of the specificities and requirements for the notifications for the relevant Union legal acts. Based~~**and reporting, including by working** on the ~~results of the piloting, the Commission should assess the proper functioning, reliability, integrity and confidentiality of the single-entry point. The Commission should consult the~~**exchange and interoperability of information regarding incident reporting. For this purpose and in cooperation with the** CSIRTs network ~~and the~~**, the Cooperation Group and** competent authorities under the relevant Union legal acts, ~~by making use of existing cooperation groups and networks of Member States established under these acts, when carrying out the assessment. Where the Commission finds that the single-entry point ensures the proper functioning, reliability, integrity and confidentiality, it should publish a notice to that effect in the Official Journal of the European Union. In case the Commission considers that the proper functioning, reliability, integrity and confidentiality is not ensured,~~ ENISA should ~~take all necessary corrective measures, followed by a reassessment by the Commission~~**develop guidelines to foster the harmonisation of incident notifications**.

~~(52) To ensure the continuity and interoperability with existing national technical solutions that facilitate incident reporting, to the extent feasible, ENISA should take into account such national technical solutions when developing the specifications on the technical, operational and organisational measures necessary to establish, maintain and securely operate the single-entry point. Further, ENISA should consider technical protocols and tools such as application programming interfaces and machine-readable standards that enable entities to integrate reporting obligations into business processes, and authorities to connect the single-entry point with their national reporting systems.~~

~~(53) To ensure that the single-entry point enables the relevant entities to submit the type of information and the format required under the relevant Union legal acts, ENISA should consult the Commission and the competent authorities under those acts. Where a Union legal act is not fully harmonized regarding the type of information and the format of notifications, Member States should inform ENISA about their national provisions.~~

~~(54) Based on Regulation (EU) 2022/2554, the financial sector has been at the forefront in implementing a harmonised, comprehensive and effective framework, including with regard to incident reporting. In order to simplify compliance, it is appropriate to align the incident reporting framework established under Regulation (EU) 2022/2554 with the single-entry point, while ensuring continuity and stability of the existing reporting framework, and considering that the single-entry point would be operational after it has been assessed that it ensures the proper functioning, reliability, integrity and confidentiality. Further, Regulation (EU) 2022/2554 has introduced standardised reporting templates streamlining the content of reports for major ICT-related incidents for the financial sector. The experience gained from the adoption of these templates provides valuable insights and best practices that should be taken into account when specifying the type of information, the format and the procedure of a notification for the purposes of reporting to the single-entry point under Directive (EU) 2022/2555, Directive (EU) 2022/2557 or Regulation (EU) 2016/679, where appropriate. For this purpose, the Commission should take due account of the regulatory technical standards adopted pursuant to Regulation (EU) 2022/2554, which specify the content of the initial notification, as well as the intermediate and final reports, concerning major ICT-related incidents. This approach aims to ensure consistency, promote synergies and reduce administrative burden on entities by minimizing the number of data fields that entities are required to complete, thereby facilitating more efficient and streamlined reporting processes.~~

(55) Under the relevant Union legal acts, certain incident-specific information is to be shared at a subsequent stage between competent authorities to facilitate effective oversight and coordination. Therefore, the ~~single-entry~~**national entry** point should be designed to accommodate and support the exchange of information at that level for each relevant Union legal act, ensuring that appropriate data flows between authorities are enabled in a secure, timely, and efficient manner, should the Member States decide to make use of this additional feature.

(56) To ensure that incident reporting is carried out via the ~~single-entry~~**national entry** point Directive (EU) 2022/2555, Regulation (EU) 2016/679, Regulation (EU) 2022/2554, Regulation (EU) 910/2014, and Directive (EU) 2022/2557 should therefore be amended accordingly. The ~~single-entry~~**national entry** point should start being used for the purpose of reporting under those acts within ~~18~~**30** months from the entry into force of this

Regulation. ~~When the Commission initiates the mechanisms of the notice delaying the date of application to 24 months from the entry into force of the Regulation, the corresponding provisions of Directive (EU) 2022/2555, Regulation (EU) 910/2014, Regulation (EU) 2022/2554 and Directive (EU) 2022/2557 should continue to apply for the purpose of meeting the reporting obligations laid down in the provisions.~~

(57) In the exceptional event that a technical impossibility prevents the submission of incident notifications using the ~~single entry~~**national entry** point, entities should fulfil their reporting obligations through alternative means. For that purpose, addressees of incident notifications under the relevant Union legal acts should ensure that they can receive such incident notifications through alternative means and should make information about that alternative means publicly available.

(58) The European Data Protection Supervisor ~~was~~**and the European Data Protection Board were** consulted in accordance with Article ~~42(1)~~**42** of Regulation (EU) 2018/1725 of the European Parliament and of the Council[8], and delivered ~~its~~**their joint** opinion on ~~[DATE].~~ ~~The European Data Protection Board was consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725 and delivered an opinion on [DATE]~~**10 February 2026**.

(59) Regulation (EU) 2019/1150 establishes a targeted set of mandatory rules at Union level to ensure a fair, predictable, sustainable and trusted online business environment within the internal market. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 provide a comprehensive regulatory framework for a safe, predictable and trusted online environments for all end-users of online services, and establish a level playing field for businesses in digital markets. In the interest of simplification of Union legislation in the field of online intermediation services and online platforms, and given that the objectives and material provisions of the Platform-to-Business Regulation are largely covered by the Digital Services Act and the Digital Markets Act, **several provisions of** Regulation (EU) ~~2019/1050~~**2019/1150** should be ~~repealed~~**deleted**. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 contribute to a fully harmonised regulatory framework for

---

8 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

digital services and digital markets, by approximating national measures concerning the requirements for providers of intermediary services and the contestability and fairness of core platforms services provided by gatekeepers. For purposes of legal certainty **and for purposes of keeping the necessary level of protection for business users**, selected definitions in Article 2, ~~the~~ provisions **on terms and conditions in Article 3,** on restrictions and suspensions in Article 4, ~~as well as~~**on ranking in Article 5, and on differentiated treatment in Article 7,** on the internal complaint-handling system in Article 11 ~~of Regulation (EU) 2019/1150 that are cross-referenced by other legal acts, in particular Directive (EU) 2023/2831 on improving working conditions in platform work, and~~**, as well as provisions in** Article 15 ensuring enforcement~~, will temporarily remain in application until the original acts are amended~~ **are maintained**.

(60) Given the technical nature of the amendments proposed in this Regulation and the urgency to deliver on a simplified legal framework, this Regulation should enter into force immediately after its publication in the Official Journal. As appropriate, transitional periods should be afforded for Member States and regulated entities to adjust to the rules.

(61) The amendments to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 are based on Article 16 TFEU. The amendments to Directive 2002/58/EC are based on Article 16 TFEU and Article 114 TFEU. All other amendments are based on Article 114 TFEU.

HAVE ADOPTED THIS REGULATION:

(...)

Article 3

Amendments to Regulation (EU) 2016/679 (GDPR)

Regulation (EU) 2016/679 is amended as follows:

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.'~~

(b) the following points are added:

'(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;~~

(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;

(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.'

(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~~ **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 interest~~**, and producing verifiable and transparent results**.'

2. 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');'

3. 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, 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 measures and the results of the assessments throughout the life cycle of the AI system.'**

4. 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 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.'

5. In Article 13, paragraph 4 is replaced by the following:

‘4. 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.**

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.’

6. In Article 13, paragraph 5 is added:

‘5. 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 legitimate interests, including making the information publicly available.’

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 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.'

(7a) In Article 25, paragraphs 1 and 2 are replaced by the following:

'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 organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, 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

organisational 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.

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~~**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 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.’

(b) the following paragraph is added:

‘1a. Until the establishment of the ~~single-entry~~ **national entry** point pursuant to Article ~~23a~~**23b** of Directive (EU) 2022/2555, controllers shall continue to notify personal data breaches directly to the competent supervisory authority in accordance with Article 55 and Article 56 **of this Regulation**.’

(c) the following paragraphs are added:

‘6. The Board shall ~~prepare and transmit to the Commission a proposal for~~ **establish and make public** a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 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 **and a list of the circumstances in which it is not likely to result in such a high risk. The template and lists**~~. The proposals~~ shall be ~~submitted to the Commission~~ **available** 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~~ **may** adopt ~~it~~ **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).

7. The template and ~~the list~~ **lists** referred to in paragraph 6 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~~ **may** adopt any updates **of the template by way of an implementing act** following the procedure **referred to** in paragraph 6.'

9. 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.

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 **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**.'

(9a) In Article 37, paragraph 7 is replaced by the following:
'7. The controller or the processor shall publish the contact details of the data protection officer.'

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 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**.

~~(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).'~~

11. ~~In~~ Article ~~57(1)~~**57** is amended as follows:

(a) **in paragraph 1,** point (k) is deleted;

(ab) paragraph 4 is replaced by the following;

'4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character or where an abusive intention on the part of the data subject submitting those requests can be demonstrated, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall, in the light of all the relevant circumstances of the case, bear the burden of demonstrating the manifestly unfounded or excessive character of the request.'

12. In Article 64(1), point (a) is deleted.

(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 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 such 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 anonymisation referred to in Article 29a.'

15. After Article ~~88~~**8**, the following ~~articles are~~ **article is** 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 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 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]~~

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 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 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 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 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.'~~

(...)

Article 5

Amendments to and Directive 2002/58/EC (ePrivacy Directive)

Directive 2002/58/EC is amended as follows:

1. Article 4 is deleted;

2. ~~After~~**In** Article ~~5(3)~~**5**, **paragraph 3 is replaced by** the following subparagraph ~~is added~~:

~~'This paragraph~~**3. Member States** shall ~~not apply if the~~ **ensure that the storing of information, or gaining of access to information already stored, in the terminal equipment of a** subscriber or user is **only allowed when that person has given his or her consent, in accordance with Regulation (EU) 2016/679.**
Storing of information, or gaining of access to information already stored, in the terminal equipment of a natural person **without consent, and subsequent processing for the same purpose, shall be lawful to the extent it is strictly necessary for any of the following purposes:**

a) carrying out the transmission of an electronic communication over an electronic communications network;

b) providing a service explicitly requested by the user;

c) creating anonymous aggregated~~, and the~~ information ~~stored or accessed constitutes or leads to the processing~~ **about the usage of an online service requested by the user to measure the audience of such a service, where it is carried out by the provider of that online service, or by a third party acting**

together with or on behalf of this provider, solely for their own use, including where the third party is performing audience measurement in accordance with Article 24 of Regulation (EU) 2024/1083;

d) maintaining or restoring the security of the interface strictly necessary for the provision of an information society service requested by the user or the security of the terminal equipment used for the provision of such service, including in particular cybersecurity, the protection of personal data **and privacy of the user and prevention of fraud;**

The user shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means. If the user gives consent, the provider 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. If the data subject refuses 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.

Member States shall designate the competent supervisory authority under Regulation (EU) 2016/679 for the supervision and enforcement of the rules under this paragraph.

2a In Article 17, the following paragraph is added:

3. Member States shall adopt and publish, by [24 months after the adoption of this Regulation] the laws, regulations and administrative provisions necessary to comply with Article 5(3). They shall immediately communicate the text of those measures to the Commission.
They should apply those measures from [24 months after the adoption of this Regulation].'

Article 6

Amendments to Directive (EU) 2022/2555

Directive (EU) 2022/2555 is amended as follows:

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 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;

(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 consult the 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 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;~~

~~(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.~~

2. The following Article 23b is added:

‘Article 23b

National entry point for incident reporting

(1) Member States shall establish and maintain a national entry point for the reporting of incidents and related events under the Union legal acts where those Union legal acts provide so. The national entry point shall enable entities to fulfil their notification obligations through a single notification at national level which reaches all relevant competent authorities.

(2) Member States shall retain flexibility to configure their national entry point in accordance with their existing competent authority structures and the allocation of competences among authorities, including by connecting existing systems and enabling the sharing, routing or distribution of relevant information.

(3) Member States shall design their national entry point with a view to make the national entry points interoperable with the national entry points of the other Member States.

(4) ENISA shall, by [12 months from the date of entry into force of this amending Regulation], in consultation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts, provide guidelines to support Member States in the establishment, maintenance and secure operation of their respective national entry point. Those guidelines shall address technical, operational and organisational measures, taking into account experiences and lessons learned from existing reporting structures. Those guidelines shall include the technical specifications necessary to ensure interoperability between all Member States’ national entry points as referred to in paragraph 3 and to facilitate the alignment of incident notifications submitted via their respective national entry point with cross-border reporting obligations.

3. The following article 23c is added :

‘Article 23c

Harmonising incident notification framework

(1) By [6 months after the entry into force of this Regulation] the Commission shall submit a report to the European Parliament and to the Council outlining common definitions, thresholds, deadlines, formats and procedures applying to Article 23 of Directive (EU) 2022/2555, Article 19a (1a), Article 24 (2a) and Article 45a (3a) of Regulation (EU) 910/2014, Article 33 (1) of Regulation (EU) 2016/679, Article 19 (1) and (2) of Regulation (EU) 2022/2554, and Article 15(1) of Directive (EU) 2022/2557.

The report shall in particular consider concrete steps and a timeline for introducing the unified approach to incident reporting under the Union legal acts.

(3) Building on the report referred in paragraph (1), ENISA shall, in consultation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts, develop guidelines to foster the harmonization of incident notifications. These guidelines shall, in particular:

(a) Identify ways to further harmonise templates for entities but also between CSIRTs across different sectors and legislative frameworks;

(b) Provide a thorough analysis on the different sectoral thresholds, and, where appropriate, provide suggestions with regards to possible harmonization to improve efficiency;

(c) Review the stages of incident notifications under different Union legal acts and recommend measures to streamline the process for entities.

ENISA shall present a first draft of these guidelines [by - within 12 months after the entry into force of this Regulation], and a final version within 18 months, and shall update them regularly thereafter.

~~(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.~~

4. The following article 23d is added:

'Article 23d

Cross-border incident notification

(1) Member States should aim at facilitating cross-border notifications to multiple national reporting structures.

(2) ENISA shall, in consultation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts, harmonise its relevant tools with national incident notification templates and facilitate an automatisation process to exchange information about cross-border impacts.

(3) Information submitted through relevant tools shall not be automatically transmitted to ENISA in full, Member States shall have the possibility to select information shared.'

2. Article 23 is amended as follows:

(a) in paragraph 1, the first sentence is replaced by the following:

'Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of this Article of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 of this Article (significant incident) via the ~~single-entry~~**national entry** point ~~established~~ pursuant to Article ~~23a~~**23b**.

The following paragraph 1b is added:

(b) ENISA shall, in cooperation with the Cooperation Group, provide a mapping of all the competent authorities and CSIRTs referred to in paragraph 1 in the single information point established pursuant to Article 23a. '

(b) the following paragraph 12 is added:

‘When a manufacturer notifies a severe incident pursuant to Article 14(3) of Regulation (EU) 2024/2847 and the incident reporting under that Article contains relevant information as required under paragraph 4 of this Article, the reporting of the manufacturer under Article 14(3) of Regulation (EU) 2024/2847 shall constitute reporting of information under paragraph 4 of this Article.;’

3. in Article 30, paragraph 1 is replaced by the following:

‘1. Member States shall ensure that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis via ~~the single-entry~~ **national entry** point ~~established pursuant to~~ **referred to in** Article ~~23a~~**23b**, by:

(a) essential and important entities with regard to incidents, cyber threats and near misses;

(b) entities other than those referred to in point (a), regardless of whether they fall within the scope of this Directive, with regard to significant incidents, cyber threats and near misses.’

Article 7

Amendment of Regulation (EU) 910/2014

Regulation (EU) 910/2014 is amended as follows:

1. in Article 19a, the following paragraph 1a is inserted:

‘1a. Notifications pursuant to paragraph 1, point (b) of this Article to the supervisory body and, where applicable, to other relevant competent authorities, shall be made through the ~~single-entry~~ **national entry** point pursuant to Article ~~23a~~**23b** of Directive (EU) 2022/2555.;’

2. in Article 24, the following paragraph 2a is inserted:

‘2a. Notifications pursuant to in paragraph 2, point (fb), of this Article to the supervisory body and, where applicable, to other relevant competent bodies, shall be made through the ~~single-entry~~ **national entry** point pursuant to Article ~~23a~~**23b** of Directive (EU) 2022/2555.;’

3. in Article 45a the following paragraph 3a is inserted:

‘3a. Notifications pursuant to in paragraph 3 to the Commission and to the competent supervisory body, shall be made through the ~~single-entry~~ **national entry** point pursuant to Article ~~23a~~**23b** of Directive (EU) 2022/2555.’

Article 8

Amendments to Regulation (EU) 2022/2554

Article 19 of Regulation (EU) 2022/2554 is amended as follows:

1. in paragraph 1, the first subparagraph is replaced by the following:

‘Financial entities shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 via the ~~single-entry~~ **national entry** point established pursuant to Article ~~23a~~**23b** of Directive (EU) 2022/2555 in accordance with paragraph 4 of this Article.’

2. in paragraph 2, the first subparagraph is replaced by the following:

‘Financial entities may, on a voluntary basis, notify via the ~~single-entry~~ **national entry** point established pursuant to Article ~~23a~~**23b** of Directive (EU) 2022/2555 significant cyber threats to the relevant competent authority when they deem the threat to be of relevance to the financial system, service users or clients. The relevant competent authority may provide such information to other relevant authorities referred to in paragraph 6.’

Article 9

Amendments to Directive (EU) 2022/2557

Article 15 of Directive (EU) 2022/2557 is amended as follows:

1. in paragraph 1, the first sentence is replaced as follows:

‘Member States shall ensure that critical entities notify via the ~~single-entry~~ **national entry** point established pursuant to Article ~~23a~~**23b** of Directive (EU) 2022/2555 the competent authority, without undue delay, of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services.;’

2. in paragraph 2, the following sub-paragraph is added:

‘The Commission may adopt implementing acts further specifying the type and format of information notified pursuant to Article 15(1). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 24(2).’

Article 10

Amendments, repeals and transitory clauses

1. Regulation 2019/1150/EU is ~~repealed with effect from [date = entry into application of this Regulation].~~ **amended as follows:**

Articles 2(11), 2(12), 6, 8 to 10, 12 to 14, and 16 to 18, are deleted as of [date of entry into force].

~~2. By way of derogation from paragraph 1, the following provisions shall continue to apply until 31 December 2032:~~

~~(a) Article 2, point (1);~~

~~(b) Article 2, point (2);~~

~~(c) Article 2, point (5);~~

~~(d) Article 4;~~

~~(e) Article 11;~~

~~(f) Article 15.~~

3. The following acts are repealed, with effect from [Date, aligned with the entry into application of the amendments]:

a) Regulation (EU) 2022/868;

b) Regulation (EU) 2018/1807;

c) Directive 2019/1024.

4. References to Regulation (EU) 2022/868, Regulation (EU) 2018/1807 and Directive 2019/1024 shall be read in accordance with the correlation table set out in Annex I of this Regulation.

Article 11

Final provisions

This Regulation shall enter into force on the third day following that of its publication in the Official Journal of the European Union.

Articles under Chapter VIIc shall enter into application 18 months after the publication in the Official Journal of the European Union.

~~Deviating from paragraph 3,~~ Article 5(2) shall enter into application 6 months after the publication in the Official Journal of the European Union.

By way of derogation from paragraph 1, Article 3(8), points (a) to (c), Articles 6 (2) and (3) and 7 to 9, shall enter into application 18 months from the entry into force of this Regulation.
~~Deviating~~**By way of derogation** from the first sentence~~, where the Commission finds in its assessment pursuant to Article 23a (7) of Directive (EU) 2022/2555 that the single-entry point does not ensure the proper functioning, reliability, integrity or confidentiality~~, the obligations to report via the ~~single-entry~~**national entry** point set out in Article ~~23(4)~~**23b** of Directive (EU) 2022/2555, Article 19a (1a), Article 24 (2a) and Article 45a (3a) of Regulation (EU) 910/2014, Article 33 (1) of Regulation (EU) 2016/679, Article 19 (1) and (2) of Regulation (EU) 2022/2554, and Article 15(1) of Directive (EU) 2022/2557 shall enter into application ~~24~~**30** months from the entry into force of this Regulation.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament
The President

For the Council
The President