Council of the European Union

Brussels, 21 September 2026
(OR. en)

13112/26

Interinstitutional File:
2025/0360 (COD)

LIMITE

SIMPL 192
ANTICI 201
DATAPROTECT 274
CYBER 366
TELECOM 420
CODEC 1657
PROCIV 175
COMPET 1059
MI 874

PUBLIC

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Proposal for a Regulation amending Regulations (EU) 2016/1679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2024/1689 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) - Presidency revised compromise text

Delegations will find attached the Presidency revised compromise text of the Digital Omnibus in view of the AGS meeting of 25 September 2026.

Additions to the Commission proposal are indicated in **bold**, deletions are marked as ~~strikethrough~~. Changes compared to the previous Presidency revised compromise text (ST 12535/26) are marked in **bold underlined**.

ANNEX

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) 2019/1150, (EU) 2023/2854, (EU) 2022/2554, and (EU) 910/2014~~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 OJ C […], […], p. […].
2 OJ C […], […], p. […].
3 OJ C […], […], p. […].

(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 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 **of** 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.

---

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

(4) Given the foundational role of data in driving value-creation in the digital economy, and pursuant to the objectives of the Communication for a European Data Union Strategy, the amendments presented in this Regulation to the legislative framework regarding data seek to build a coherent and cohesive regulatory framework for the availability and use of data, streamlining and consolidating the data regulatory framework into only two legal acts, namely Regulations (EU) 2016/679[5] and (EU) 2023/2854[6] of the European Parliament and of the Council, from currently five different applicable acts. The amendments seek to cut unnecessary administrative costs and stimulate the availability of data as a prerequisite for supporting competitive digital businesses in the Union, while maintaining the highest standard of protections for privacy, personal data protection, and fair business practices, and ensuring core regulatory objectives, including compliance with EU and national competition law.

(5) Acknowledging the iterative evolution of horizontal and sector-specific rules, it is indispensable to address also overlaps in specific provisions that result in unnecessary duplications of administrative burdens. This is the case in requirements across several rules for reporting following cybersecurity and related incidents, where digital solutions~~, as proposed in this Regulation,~~ can bring an immediate relief to businesses across all concerned sectors.

(6) Similarly, with the iterative regulation of online platforms over the past years, more recent rules have established a clearer and more ambitious framework than some of the predating rules, rendering them obsolete. It is therefore necessary that the legal framework evolves, eliminating any unnecessary duplications that add legal complexity.

---

5 REGULATION (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

6 REGULATION (EU) 2023/2854 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)

(7) Regulation (EU) 2022/868 of the European Parliament and of the Council[7] has established rules for intermediary functions in three different settings: (a) functions that support the re-use of protected data held by public sector bodies under controlled conditions; (b) data intermediation services that facilitate data sharing between data subjects, data holders and data users; and (c) data altruism organisations that support the use of data made available by data subjects and data holders on an altruistic or philanthropic basis. Functions supporting the re-use of protected data held by the public sector have a close link with rules of Directive (EU) 2019/1024 of the European Parliament and of the Council[8]. Their interplay has caused confusion namely among public sector bodies. It is thus necessary to merge the two sets of rules. The evaluation of the rules on data intermediation services has shown that the definition of data intermediation service providers has weaknesses and that the rules are overly stringent for service providers to find a sustainable financial model. It is thus also necessary to streamline the regime. With respect to data altruism, certain rules of Regulation (EU) 2022/868, notably the obligation on Member States to have national policies on data altruism in place, the establishment of a 'rulebook' and developing a European data altruism consent form appear unnecessary regulation, also in light of on-going work by the European Data Protection Board referred to in Article 68 of Regulation (EU) 2016/679 of the European Parliament and of the Council[9] on guidance on the processing of personal data in the context of scientific research.

(8) While the importance of data intermediation services is recognised in the context of many initiatives supporting data sharing and collaboration, the rules of Regulation (EU) 2022/868 on data intermediation service providers should be clarified. In particular, the definition of such providers should be made more precise. It should eliminate elements that served merely as illustrative examples, rather than exceptions. Moreover, it should address loopholes resulting from ambiguous formulations, notably as regards the notion of 'closed

---

7 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (OJ L 152, 3.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/868/oj).

8 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (OJ L 172, 26.6.2019, p. 56, ELI: http://data.europa.eu/eli/dir/2019/1024/oj).

9 Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

group'. Services should not be eligible to register as data intermediation services where they are exclusively used by a closed group of companies and where any extension of that group of companies can only be decided by that group and not the service provider. More importantly, making this emerging market subject to a compulsory regime has created unnecessary compliance costs. At this stage of market development, a voluntary regime, allowing neutral players to distinguish themselves from other players, appears sufficient. Also, in order to enable sustainable business models, the regime should be made less strict by abolishing the requirement for a legal separation between data intermediation services and other value-added services that a **data intermediation** service **provider** should be allowed to offer, replacing it with a functional separation while keeping certain safeguards. The administrative monitoring regime should be simplified. Instead of national and a Union public register for data intermediation services providers and data altruism organisations, there should only be Union public registers, namely one for data intermediation service providers and another for data altruism organisations. Competent authorities overseeing the award of the label and the compliance of the entities with the requirements for obtaining it should be independent in this task. This should be understood to mean that they are legally and functionally independent from a data intermediation service or data altruism organisation, including at the level of their top-management. It should be possible for government organisations to financially support data intermediation services or data altruism organisations, in particular given the emerging nature of these entities, provided that they are legally separate entities. In order to ensure that recognised entities are easily identifiable throughout the Union, the Commission established Implementing Regulation (EU) 2023/1622 ~~**on the design of common logos to identify data intermediation services providers and data altruism organisations recognised in the Union**. on the design of common logos to identify data intermediation services providers and data altruism organisations recognised in the Union.~~

(9) Regulation (EU) 2023/2854 removes barriers to data access and use, unlocks data-driven innovation and competitiveness, and safeguards the incentives of those who invest in data technologies.

(10) Chapter II of Regulation (EU) 2023/2854 requires data holders to make data available, including data protected as trade secrets, to users and their selected third parties, provided confidentiality measures established by the data holder are maintained. This requirement of maintaining confidentiality complements Directive (EU) 2016/943 of the European

Parliament and of the Council [10], which sets the standard for protecting trade secrets within the Union. However, disclosure of trade secrets to third-country entities may increase risks to their integrity and confidentiality where there is exposure to jurisdictions with inadequate protections or difficulties in their actual enforcement, potentially resulting in unauthorised use, economic damage and legal uncertainty.

(11) It is necessary to strengthen Regulation (EU) 2023/2854 by introducing an additional ground for data holders to refuse **access to data where such access could lead to** the disclosure of trade secrets, supplementing existing provisions which allow refusal based on the data holder's demonstration of a ~~high~~ likelihood of serious economic damage. Under the new provision, data holders may refuse **a request to access to data**~~to disclose trade secrets~~ if they demonstrate a high risk of unlawful acquisition, use, or disclosure to entities subject to regimes with inadequate protection, non-equivalent, or weaker legal frameworks than the applicable Union rules. The new provision also covers instances where the third country legal framework, in theory, is robust or exceeds such Union rules, but lacks appropriate enforcement in practice. Such risks highlight the possibility that trade secrets could be acquired, used, or disclosed in violation of Union law, threatening the integrity and confidentiality of trade secrets.

(12) The activation of the refusal mechanism should remain voluntary, and the demonstration done only upon its activation. Data holders should not be required to conduct a full-scale analysis or demonstration of the level of trade secret protection in third countries or by a third country entity as a precondition to be able to substantiate their refusal to sharing data or to disclose trade secrets. In their demonstration, data holders may take into consideration various factors, such as insufficient or inadequate legal standards, poor or arbitrary enforcement, historical infringements, foreign disclosure obligations conflicting with Union law, limited legal recourse or remedies for Union entities, the strategic misuse of procedural tactics to undermine competitors, or undue political influence. Given the diverse range of entities, third countries, and data sharing scenarios involved, data holders should focus their assessment and demonstration on pertinent risks and act accordingly, including by setting appropriate safeguards or activating the refusal mechanism. Refusals

---

[10] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (OJ L 157, 15.6.2016, p. 1).

should be clear**,** **and** proportionate~~, and tailored to the specific circumstances of each case, rather than being applied systematically or in a generalized manner across entities of an entire third country~~.

(13) An insufficient protection of trade secrets and the challenges in enforcing **it** ~~them~~ in third countries may cause irreparable harm to European businesses. The objective is therefore to strengthen the safeguards for trade secrets by preventing their leakage to natural or legal persons that are established in or subject to jurisdictions posing such risks. This includes Union-based entities controlled by third country entities, who may be acting in bad faith or as fronts for third country entities. Additionally, the objective is to avert direct exposure to third country entities operating within the Union, that are subject to such jurisdictions. Being subject to a third country jurisdiction means the natural or legal person is legally governed, controlled or otherwise bound by the laws or regulatory authority of a third country. Subsidiaries or affiliates of third country ~~parent~~ companies may exploit these jurisdictions to evade or circumvent Union laws. Direct or indirect control refers to the ability to exercise decisive or dominant influence over another entity's management or strategic decisions, whether through ownership of capital or voting rights, financial participation, contractual arrangements, or intermediary entities. Control may be exercised directly or through other means, even without majority ownership. Data holders should use best efforts to obtain the relevant information, which may include searches in public registers or requesting it from the user or third party directly, while ensuring it remains appropriately non-intrusive.

(14) Protecting trade secrets from those vulnerabilities is essential for European~~ industries~~ **businesses** to sustain their market position and competitive advantage. While data holders may exercise discretion in protecting their trade secrets, refusals to share data should be limited to justified, exceptional circumstances, in order to preserve the objectives of Regulation (EU) 2023/2854 of fostering data-driven innovation and a thriving digital economy in the Union. Safeguards against misuse of the refusal mechanism should remain in place, including the data holder's obligation to demonstrate in a duly substantiated manner that disclosure poses a high risk and to notify competent authorities. This demonstration should be provided in writing without undue delay to the user or third party and proportionate to the case at hand. All parties involved should treat the decision and supporting demonstration as confidential in order to uphold the confidential nature of the trade secrets concerned. Users and third parties, as the case may be, may challenge the data

holder's decision with the competent authority, in court, or through dispute settlement bodies.

(15) To simplify the business-to-government data sharing framework under Regulation (EU) 2023/2854 and to clarify ambiguities that previously imposed broader obligations on businesses, it is necessary to narrow the scope of Chapter V of that Regulation from 'exceptional need' to 'public emergencies'. The concept of 'public emergencies', which is defined under Article 2(29) of Regulation (EU) 2023/2854, ~~thus~~ ensures that the obligations laid down in that Chapter are invoked only **in**~~under~~ well-defined, urgent situations**, which are unforeseeable and limited in time**, reducing the technical, administrative and legal challenges that **businesses**~~business~~ faced under the previous regime. This would ensure that data requests are relevant and proportionate to responding, ~~mitigating,~~ or supporting the recovery from public emergencies**. While 'responding to' a public emergency presupposes an ongoing public emergency, which has been determined or officially declared in accordance with the relevant procedures under Union or national law, 'supporting the recovery from' a public emergency covers measures undertaken after the public emergency has been determined or officially declared over. The third alternative of 'mitigating' a public emergency under Regulation (EU) 2023/2854 should be deleted because it is already covered by the notion of 'responding to' public emergencies. Given that the scope of Chapter V is narrowed substantially and to simplify the request mechanism, a body requesting data to 'support the recovery from' a public emergency should not be obligated anymore to exhaust all other means at its disposal to obtain such data before launching the request, such as purchasing the non-personal data on the market by offering market rates. Instead, it should be sufficient that the requesting body was unable to otherwise obtain the data in a timely and effective manner and under equivalent conditions**. Since the updated Union framework on European statistics under Regulation (EC) No 223/2009 of the European Parliament and of the Council[11] does not

[11] Regulation (EC) **No 223/2009**~~No 223/2009~~ of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) **No 1101/2008**~~No 1101/2008~~ of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) **No 322/97**~~No 322/97~~ on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the

address public emergencies, it is essential to preserve the role of official statistics under Chapter V of Regulation (EU) 2023/2854 to ensure clarity and effectiveness **when the production of official statistics is required to respond to or support the recovery from a public emergency**~~in such situations~~. It is also necessary to clarify the compensation regime for situations where microenterprises and small enterprises are required to provide data to **respond to**~~address~~ a public emergency, in which case such enterprises are allowed to claim compensation.

(16) In order to mitigate legal uncertainties that could discourage innovative business models, it is necessary to address the substantial compliance ambiguities and burdens associated with the provisions on smart contracts executing data sharing agreements under Article 36 of Regulation (EU) 2023/2854. The absence of harmonised standards and clear definitions for key concepts such as 'robustness', 'access control', and 'consistency with contractual terms', combined with the requirement for a 'safe termination or interruption mechanism' potentially incompatible with decentralised or public blockchain architectures built on immutable ledgers, posed challenges to innovators from a cost and opportunity perspective. Additionally, the ambiguity surrounding the performance of the conformity assessment under Article 36(2) of that Regulation risks imposing disproportionate burdens. The elimination of Article 36 of Regulation (EU) 2023/2854 would therefore promote the development and market introduction of new business models, foster innovation, and reduce barriers for emerging technologies.

(17) Certain data processing services, which do not fall within the Infrastructure as a Service (IaaS) delivery model, are ~~adapted~~custom-made to the needs or ecosystem of a customer. The provision of such data processing services is based on time-intensive pre-contractual and contractual negotiations to determine the specific requirements of the customer and subsequent technical efforts to customise the data processing service and to deliver a tailored solution. Those are services not provided off-the-shelf and are personalised to the needs of a customer to provide a tailored solution where the majority of features and functionalities of the data processing service has been adapted by the provider to the specific needs of the customer ~~where the majority of features and functionalities would~~

European Communities (OJ L 87, 31.3.2009, p. 164, ELI: http://data.europa.eu/eli/reg/2009/223/oj).

~~not be usable for a customer without prior adaptation by the provider~~. Those services differ from custom-built data processing services referred to in Article 31(1) of Regulation (EU) 2023/2854. Custom-built data processing services are services of which the majority of main features has been custom-built to accommodate the specific needs of an individual customer or where those data processing services are not offered at broad commercial scale via the service catalogue of the provider. To avoid additional costs and administrative burden connected to the need to reopen and renegotiate contracts concluded before or on 12 September 2025, it is necessary to clarify that, with the exception of the obligation to reduce and ultimately remove switching and egress charges, ~~those adapted~~custom-made services provided according to contracts concluded before or on 12 September 2025 should not fall within scope of Chapter VI of Regulation (EU) 2023/2854.

(18) For reasons relating to financial planning and attracting investment, providers of data processing services, especially SMEs and SMCs, may prefer and offer contracts of a fixed duration. It is necessary to clarify that providers of data processing services may include provisions on proportionate early termination penalties in those contracts as long as they do not constitute an obstacle to switching. In addition, providers of data processing services that are SMEs or SMCs are particularly burdened by the need to align existing contracts for the provision of data processing services to Regulation (EU) 2023/2854. It is therefore necessary to establish a specific regime for those providers if they provide data processing services, other than IaaS, based on contracts concluded before or on 12 September 2025. Taking into account the aim of Regulation (EU) 2023/2854 to enable switching between data processing services and given that switching charges, including egress charges, constitute a serious obstacle to switching, the new lighter regimes for data processing services that are custom-made or are provided by SMEs or SMCs should not undermine the gradual withdrawal of those charges. Contractual provisions running contrary to that objective should be considered to never have existed, if they are included in contractual agreements on the provision of services falling within the scope of those two new specific regimes.

(19) Regulation (EU) 2018/1807 of the European Parliament and of the Council[12] introduced a key principle for supporting the data-driven economy within the Union, underpinning in concrete terms the freedom of establishment and freedom to provide a service. 'Free flow of data' **within**~~in~~ the Union, clarified through the prohibition to impose data localisation, remains a fundamental principle, providing legal certainty to businesses, and should be retained in Regulation (EU) 2023/2854**. The Commission should continue monitoring deviations from this principle**. The provision does not affect the data processing in so far as it is carried out as part of an activity which falls outside the scope of Union law, in particular as regards national security, in accordance with Article 4 of the Treaty on European Union. At the same time, other provisions of Regulation (EU) 2018/1807 are superseded by more recent rules. Notably, Chapter VI of Regulation (EU) 2023/2854 introduced a modern horizontal legal framework addressing switching between data processing services and rendered Article 6 of Regulation (EU) 2018/1807 practically obsolete. The co-existence of those provisions has increased legal complexity for businesses. Therefore, Regulation (EU) 2018/1807 should be repealed.

(20) The concept of 'public security', within the meaning of Article 52 TFEU and as interpreted by the Court of Justice, covers both the internal and external security of a Member State, as well as issues of public safety, in order, in particular, to facilitate the investigation, detection and prosecution of criminal offences. It presupposes the existence of a genuine and sufficiently serious threat affecting one of the fundamental interests of society, such as a threat to the functioning of institutions and essential public services and the survival of the population, as well as the risk of a serious disturbance to foreign relations or the peaceful coexistence of nations, or a risk to military interests. In compliance with the principle of proportionality, data localisation requirements that are justified on grounds of public security should be suitable for attaining the objective pursued, and should not go beyond what is necessary to attain that objective.

(21) Both Directive (EU) 2019/1024 and Chapter II of Regulation (EU) 2022/868 regulate the re-use of public sector information for innovation purposes. The interplay of the two sets of rules has created legal uncertainty, mainly for public sector bodies. An alignment of the

---

[12] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (OJ L 303, 28.11.2018, p. 59, ELI: http://data.europa.eu/eli/reg/2018/1807/oj).

rules in one legal instrument is therefore necessary to bring further legal coherence and certainty.

(22) Since both Directive (EU) 2019/1024 and Regulation (EU) 2022/868 share the goal of enhancing the re-use of public sector information, and **in**~~inn~~ order to simplify rules from the perspective of both public sector bodies and of re-users of public sector information, it is rational to repeal Directive (EU) 2019/1024 and Regulation (EU) 2022/868**,** and align the two regimes and consolidate the rules in a single Chapter under this Regulation **(EU) 2023/2854**. This solution will increase harmonisation of those rules across the Union, reduce the administrative burden associated with interpreting and implementing national legislation and make it easier for businesses to develop cross-border services and products. ~~When designating competent bodies, Member States should ensure that even where sector-specific competent bodies are designated, all relevant sectors are ultimately covered.~~ The amendments in this Regulation should be understood not to alter the interpretation of the different definition and terms, unless clearly specified. **However, the consolidation respects and allows to maintain national organisational specificities to ensure flexibility for national, regional and local administrations. To this end, the minimum harmonisation for data and documents in scope of Section II of Chapter VIIc should ensure that Member States are able to adopt policies, practical arrangements and rules that exceed the minimum standards laid down for such data and documents, thus allowing for more extensive re-use.**

(22a) It should be recalled that the intellectual property rights of third parties are not affected by Chapter VIIc. The term 'intellectual property rights' refers to copyright and related rights, including sui generis forms of protection, and to industrial property rights, such as patents and registered designs and trademarks. Chapter VIIc Section 2 does not apply to data and documents covered by intellectual property rights of third parties, including industrial property rights such as patents and registered designs and trade marks. Chapter VIIc Section 3 applies to data protected on the ground of intellectual property rights of third parties, including on the grounds of industrial property rights. Provisions of Chapter VIIc Section 3 of Regulation (EU) 2023/2854 oblige public sector bodies to ensure that re-use does not affect the protected nature of those data.

(23) Data and documents, which can be made publicly available for reuse, and data ~~and documents~~, which are protected on the grounds of commercial confidentiality, including business, professional and company secrets, statistical confidentiality, the protection of intellectual property rights of third parties or the protection of personal data, are often held by the same public sector bodies. Therefore, it is necessary to align definitions and common principles applying to all public sector information and **to** address questions regarding the interplay of the two sets of rules.

(24) The existing rules should be streamlined to enhance clarity and consistency. Nevertheless, the two reuse regimes should remain distinct and their respective scope of application should continue to depend on the characteristics of the data or documents and the context of their reuse. Public sector bodies should apply the open data regime whenever possible. Only where they determine that data ~~or a document~~ contains information corresponding to certain categories of protected data**,** should they limit its public availability and consider making it available for reuse as protected data.

(24a) The consolidation of the rules should in particular maintain the principle that the rules under Section 3 of Chapter VIIc should not create an obligation to allow the re-use of certain categories of protected data held by public sector bodies. In particular, Member States should therefore be able to decide whether such protected data is made accessible for re-use, also in terms of the purposes and scope of such access. The rules under Chapter VIIc Section 3 should complement and be without prejudice to more specific obligations on public sector bodies to allow re-use of protected data laid down in sector-specific Union or national law. Public access to official documents may be considered to be in the public interest. Taking into account the role of public access to official documents and transparency in a democratic society, Chapter VIIc of Regulation (EU) 2023/2854 should also be without prejudice to Union or national law on granting access to and disclosing official documents. Access to official documents may in particular be granted in accordance with national law without imposing specific conditions or by imposing specific conditions that are not provided by Chapter VIIc Section 3 of Regulation (EU) 2023/2854.
The re-use regime provided for under Section 3 of Chapter VIIc should apply to protected data the supply of which forms part of the public tasks of the public sector bodies concerned under law or other binding rules in the Member States. In the absence of such rules, the public tasks should be defined in accordance with common

PUBLIC

administrative practice in the Member States, provided that the scope of the public tasks is transparent and subject to review. The public tasks could be defined generally or on a case-by-case basis for individual public sector bodies. The protected data held by public undertakings should not be covered by Chapter VIIc Section 3 of Regulation (EU) 2023/2854. Protected data held by cultural establishments, such as libraries, archives and museums as well as orchestras, operas, ballets and theatres, and by educational establishments should not be covered by the rules under Section 3 of Chapter VIIc, since the works and other documents they hold are predominantly covered by third party intellectual property rights. Research-performing organisations and research-funding organisations could also be organised as public sector bodies or bodies governed by public law. The rules relating to protected data should apply to such hybrid organisations only in their capacity as research-performing organisations. If a research-performing organisation holds protected data as a part of a specific public-private association with private sector organisations or other public sector bodies, bodies governed by public law or hybrid research-performing organisations, i.e. organised as either public sector bodies or public undertakings, with the main purpose of pursuing research, those protected data should also not be covered by the rules governing the re-use of protected data. Where relevant, Member States should be able to apply the rules on protected data under Section 3 Chapter VIIc to public undertakings or private undertakings that exercise public sector duties or provide services of general interest. The exchange of protected data, purely in pursuit of their public tasks, among public sector bodies in the Union or between public sector bodies in the Union and public sector bodies in third countries or international organisations, as well as the exchange of protected data between researchers for non-commercial scientific research purposes, should not be subject to the provisions concerning the re-use of certain categories of protected data held by public sector bodies.

(24b) **Member States should establish a single information point as an interface for re-users seeking to re-use specific categories of protected data held by public sector bodies. The single information point should have a cross-sector remit, complement sectoral arrangements where necessary, and may rely on automated means to transmit enquiries or requests for re-use, subject to appropriate human oversight. Existing arrangements, such as open data portals, may be used for that purpose. It should**

PUBLIC

maintain an asset list providing an overview of available data resources, including, where relevant, data resources accessible through sectoral, regional or local information points, together with relevant descriptive information. Member States should also designate, establish or facilitate the establishment of one or more competent bodies to support public sector bodies in enabling the re-use of protected data. Such bodies may, where provided for under Union or national sectoral law, grant access to data. They should assist public sector bodies by providing expertise on state-of-the-art techniques for structuring, storing and making data accessible, including through application programming interfaces, and for ensuring interoperability, transferability and searchability. They should also support the use of best practices, applicable regulatory and technical standards, and secure processing environments that enable data analysis while preserving privacy, confidentiality and other protected interests. Competent bodies should act in accordance with the instructions of the public sector body concerned. They may also support data subjects and data holders in managing consent or permissions for re-use, including for scientific research conducted in accordance with recognised ethical standards. Without prejudice to the powers of data protection authorities, any processing of personal data should remain under the responsibility of the public sector body responsible for the relevant register, which remains the controller within the meaning of Regulation (EU) 2016/679. Member States should be able to designate one or more competent bodies, including internal services of public sector bodies. A competent body may assist other public sector bodies in enabling re-use of data or may itself enable such re-use. Assistance may include providing guidance on compliance with the rules relating to re-use of protected data, including on secure processing environments and technical measures to ensure privacy and confidentiality. Where competent bodies grant or refuse access for the re-use Articles 32k, 32w, 32x, 32y and 32ab should apply to those competent bodies.

(25) Start-ups, small enterprises and enterprises that qualify as medium-sized enterprises under **point**~~Article~~ 2 of the Annex to Commission Recommendation 2003/361/EC[13] and

[13] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

enterprises from sectors with less-developed digital capabilities struggle to re-use data and documents. At the same time a few very large entities have emerged with considerable economic power in the digital economy through the accumulation and aggregation of vast volumes of data and the technological infrastructure for monetising them. Those very large enterprises include undertakings that provide core platform services and are designated as gatekeepers under Regulation (EU) 2022/1925 of the European Parliament and of the Council[14] and subject to special obligations to address the imbalances. To address those imbalances and strengthen competition and innovation, public sector bodies should be able to introduce special conditions in licences pertaining to the re-use of data and documents by very large enterprises. **Member States may further specify the criteria for what constitutes a very large enterprise for the purpose of Regulation (EU) 2023/2854.** Any such conditions should be proportionate, be based on objective criteria, taking into consideration the economic power, the entity's ability to acquire data or the designation as a gatekeeper under Regulation **(EU)**~~€~~ 2022/1925, other such criteria, where appropriate. Such special conditions may, inter alia, pertain to the charges and fees or the purposes of re-use.

(26) In the spirit of fostering innovation and maintaining fair competition within the Union's digital market, it is imperative to ensure that access to and reuse of public sector **information**~~data~~ benefit a wide range of market participants and do not inadvertently reinforce existing dominant positions. Very large enterprises, and in particular undertakings designated as gatekeepers under Regulation (EU) 2022/1925, hold significant power and influence over the internal market. To prevent such entities from leveraging their substantial means to the detriment of fair competition and innovation, public sector bodies should be able to set out higher charges and fees for the re-use of **public sector** open ~~government~~ data and protected data. Such higher charges and fees should be proportionate and should be based on objective criteria, taking into consideration the economic power and the entity's ability to acquire data. This measure serves to safeguard

---

[14] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj).

opportunities for smaller businesses and new market entrants to innovate and compete in the digital economy.

(26a) **While Member State are required to designate one or more competent authorities to be responsible for the application and enforcement of Regulation (EU) 2023/2854 (competent authorities), uncertainty persists about the role of supervisory authorities responsible for monitoring and enforcement of Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 under Regulation (EU) 2023/2854. Regulation (EU) 2023/2854 recalls that Regulation (EU) 2016/679 applies to the processing of personal data by private and public authorities of the Member States and Regulation (EU) 2018/1725 applies to the processing of personal data by all Union institutions and bodies when these organisations are data holders, data users or third parties under this regulation. It further stipulates that the powers and competences of supervisory authorities under Regulation (EU) 2016/679 and (EU) 2017/1725 remain unaffected by Regulation (EU) 2023/2854. In addition, the current rules of Regulation (EU) 2023/2854 state that these authorities are responsible for monitoring the application of Regulation (EU) 2023/2854 insofar as the protection of personal data is concerned and impose fines for the infringement of this regulation. To clarify the role and responsibilities of the supervisory authorities responsible for monitoring and enforcing Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 when personal data are processed pursuant to this regulation and to increase legal certainty, it is necessary to amend Regulation (EU) 2023/2854 by ~~deleting~~clarifying that the supervisory authorities responsible for monitoring the application of Regulation (EU) 2016/679 should be responsible for monitoring the application of Regulation (EU) 2023/2854 insofar as the protection of personal data is concerned. As a consequence of this clarification, Articles ~~37(3) and~~ 40(4) and (5) of that Regulation should be deleted.**

(26b) **The European Data Innovation Board's character as a consultative body as regards the implementation and the enforcement of the Data Act should be maintained. However, its structure should be simplified and should allow for more strategic discussions. Notwithstanding these changes, the Board should continue to serve as a forum to develop consistent practice of competent authorities in the enforcement of Chapters II, III, V and VII, VIIa and VIIc. To this end, technical exchanges relating to best practices and dialogue between national enforcement bodies, including information sharing shall continue to be possible in various subgroups. These**

subgroups should also be able to discuss matters relating to the newly added Chapters VIIa and VIIc. The European Data Innovation Board should also be consulted on guidelines the Commission may issue to support the sectorial implementation of the Data Act.

(26c) The special provision of the Data Act on the right to lodge a complaint and the right to an effective judicial remedy should not apply to Chapters VIIb and VIIc. It is clarified that this is without prejudice to any rights or obligations stemming from the Charter of Fundamental Rights.

(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 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[15]. 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) **Pseudonymisation is one of the possible** ~~security~~ **measures within the meaning of** **Article 25 and** **Article 32 of Regulation (EU) 2016/679 and does not necessarily have to be applied in all cases**~~. Its legal effect should depend upon its actual effectiveness in preventing identification of a natural person by the relevant recipient~~**. Controllers and processors should remain free to use other equally effective or more effective technical and organisational measures capable of achieving the substantive confidentiality, integrity and data-protection outcomes required by this Regulation. 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. It is important that Member States, supervisory authorities, the Board and the Commission support and encourage the drawing up of such codes of conducts with regard to the pseudonymisation of personal data. Apart from pseudonymisation, other privacy-enhancing technologies could be applied as appropriate.**

(27b) **In light of the interpretation provided in the** ~~case-law~~**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,~~**third party, as**

~~15~~ ~~**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)**~~

well as when such ~~recipient~~**a third party** further discloses, transmits or otherwise makes such data available to ~~a~~**another** third party. **Pseudonymisation may, depending on the circumstances of the case, 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.**

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, such as singling out or online identifiers. A third party who processes the pseudonymised data should not be considered to have access to such means, if the likelihood of identification appears in reality to be insignificant, because it would be impossible to do or would involve disproportionate effort in terms of time, cost and labour, or because of a legal prohibition. The identifiability of a natural person should be assessed considering the actual technical and organisational measures, and based on objective factors, including legal obligations and ~~applicable~~ **prohibitions by law applicable to the third party. These factors may also include the state of the art of the techniques used to pseudonymise the data, the properties of the data itself, and the cost and time needed for the third party to obtain such additional information** ~~and the legal obligations~~**. It is important to recall that, for a controller applying pseudonymisation or a processor processing on behalf of the** ~~third party. Data which are in themselves impersonal~~**controller, the data subject remains identifiable and therefore Regulation (EU) 2016/670 applies. Data may become 'personal'** ~~in nature~~ **where they are put at the disposal of other persons who have means reasonably likely to enable the data subject to be identified. This applies to both the party that transmits this data and the third party that subsequently processes this data. Whether means are reasonably likely to be used will depend on the relevant** ~~entity's perspective~~**circumstances, which** ~~depends on~~**include the specific nature and context of the processing**~~,~~ **such as who has access to or control over the data, whether the data is being transmitted from one party to another, the relationship between those parties, and whether a receiver of the data might process it on behalf of another party.**

(27c) The European Data Protection Board should ensure consistency and support organisations 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 organisations regarding the effective application of pseudonymisation to personal data.

(28) In order to assess whether **scientific** research **activities meet**~~meets~~ 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**~~in the specific area.~~**research**~~Research~~**integrity. Transparency could, 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**~~and technology development~~ 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. The fact that scientific research activities

are to be conducted autonomously and independently does not exclude that such activities can be mandated and conducted by public authorities or private entities, including small and medium sized undertakings, in academic, industry and other settings **. 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~~, including small and medium-sized undertakings, (Article 179(2) TFEU) and~~ should be **assessed and substantiated by the controller on a case-by-case basis, considering the objective characteristics of the research activity,**~~always of a of high quality~~ and should **not undermine the obligation to apply appropriate safeguards as provided for in Article 89 of Regulation (EU**~~ adhere to the principles of principles of reliability, honesty, respect and accountability (verifiability~~) **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 **should not be**~~is not~~ 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, and should be 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 **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**~~therefore pursues a~~ legitimate **interests pursued by a controller or by a third-party**~~interest~~ 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, **which can include**~~including~~ personal data and special categories thereof. Special categories of personal data may ~~unintentionally~~**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 intend to process such personal data and has taken the appropriate technical and organisational measures to avoid such processing, such as the filtering out of special categories of personal data at the collection stage.**

~~.~~In order not to disproportionately hinder the development and operation of AI and taking into account the capabilities of the controller to identify and **erase**~~remove~~ special categories of personal data**, including technical capabilities**, derogating from the prohibition on processing special categories of personal data under Article 9(2) of Regulation (EU) 2016/679 should be **limited to incidental and residual processing of special categories of data in the context of the development and technical operation of AI systems or AI models. The derogation should not be understood as covering the processing of special categories of personal data directly acquired by or provided to the AI system or AI model in the course of the deployment**~~allowed~~. 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 **throughout**~~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 **erase them. If erasure**~~remove them. If removal~~ would **prove technically impossible or** require **manifestly** disproportionate effort, notably where the **erasure**~~removal~~ 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 **for example if special categories of personal data relating to a natural person's voice, image or other personal**

characteristics are used in a way that goes beyond incidental or residual existence. 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 carried out for a legitimate interest of the controller concerned in accordance with Article 6(1)(f) of Regulation 2016/679, where appropriate, except 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, or where other Union or national laws explicitly require consent. This does not affect the obligation of the controller to choose an 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. Regardless of the lawful ground of processing, any such processing should be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to respect data minimisation during the stage of selection of sources, and to protect against non-disclosure of residually retained data in the AI system or AI model. Other provisions of this Regulation remain unaffected by the fact that a controller relies on this legal basis.**

(34) **Processing of biometric**~~**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. **Processing**~~**The notion**~~ of biometric data **could be carried out for**~~**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** ~~appropriate~~**applicable, safeguards** ~~are~~ **laid down in Union law or national law adopted in accordance with Article 9(4) of Regulation (EU) 2016/679**~~, subject to those safeguards~~**. 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 example, such safeguards could include technical and organisational measures ensuring that original biometric samples of the data subject cannot be reconstructed from the template stored on a device or a database.**

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 **ensure that the biometric data or the means needed for the verification are under the**~~enable the data subject to have~~ sole control of the **data subject. Sole control means that the data subject can effectively decide when 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 **device**~~side~~ of the data subject or are securely stored **by**~~at the side of~~ 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, **and subject to measures ensuring the overall security of**~~that~~ processing**, including during the enrolment phase of the data subject's** ~~is not likely to create significant risks to his or her fundamental rights and freedoms. The controller does not gain knowledge of the~~ biometric data **and**~~or only for a very limited time~~ 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 **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**~~of access, which is from the outset favourable to data subjects,~~ should **provide**~~not be abused in the sense that~~ the 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**~~subjects abuse them for purposes other than the protection of their data~~. For example, such an **abusive intention**~~abuse of the right of access~~ would arise where the data subject **submits**~~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~~ excessive **numbers of identical or largely similar requests**~~use of the right of access~~ with the **sole**~~only~~ intent of causing damage or harm to the controller**. 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**~~ or when~~ an individual **submits**~~makes~~ 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 a subject submits** a request **with the sole purpose of obtaining compensation for an alleged infringement**~~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,~~ which **is deliberately provoked by**~~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~~ the data subject**, or**

when the exercise of a right is made with the intention to adversely affect and burden public authorities, for instance by utilising AI agents for malicious automated ~~should be as specific as possible. Overly broad and undifferentiated~~ requests ~~should also be regarded as excessive~~.

(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. Repeated requests are not automatically excessive in nature but may indicate an abusive intent on the part of the data subject. 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 **that**~~the~~ Regulation, this derogation should be extended to situations **such as when the personal data have been collected in the context of a direct and clearly 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 **that**~~the~~ Regulation, and there are reasonable grounds to **believe**~~assume~~ 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**. For example, there can be reasonable grounds to believe that the data subject already has such**

information in a direct and clearly circumscribed~~, in particular regarding the relationship between data subjects and the controller. These should be the situations where the context of the~~ relationship**, established for instance where** ~~between~~ the controller and the data subject **interact directly in a specific occasion**~~is very clear and circumscribed and the controller's activity is not data-intensive~~, 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 **cases**~~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~~, 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 **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**~~for~~ 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 **when assessing whether a decision**~~decisions~~ 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**~~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 **establish and make public**~~prepare 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**, and a common list of circumstances in which a personal data breach does not result in such a high risk. To further facilitate compliance, the Board should prepare a common template for notifying data breaches to the competent supervisory authority**. The Commission should take due account of the proposal prepared by the Board and review **it**~~them~~, as necessary, prior to adoption **by means of an implementing act.** ~~.~~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 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) of Regulation (EU) 2016/679. The common lists 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 and in which a personal data breach is not likely to result in a high risk should also apply in order to determine when communicating the data breaches to the data subject, in accordance with Article 34.**

PUBLIC

(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 the extent it relates to their own obligations under that Regulation. This obligation does not affect the level of responsibility and relationship between the controller and processor, nor does it affect the principle of accountability or the respective obligations of controller and processor as laid down under Article 28 of Regulation (EU) 2016/679). Accordingly, the controller remains solely responsible for determining the purpose and means of processing and for complying with related obligations, while the processor should ensure that data protection by design and by default is applied to its offered means and services to carry out processing.**

(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 **established and made public**~~prepared~~ by the Board**. 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** ~~and adopted by the Commission as an implementing act~~. In order to facilitate compliance by controllers, the Board should also prepare 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 **by mean of an implementing act**. 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.

(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 or repealing 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. The consistent application of Regulation (EU) 2016/679 should also contribute to innovation and competitiveness of the Union.

(40b) Further, in view of the consistent application of that Regulation, it is recalled that transfers of personal data to a third country or an international organisation are not required to be non-repetitive in order to fulfil one of the derogations of Article 49(1), points (a) to (g), of Regulation (EU) 2016/679. Therefore, the derogation in point (d) of that provision allows for transfers of personal data which are necessary for important reasons of public interest, even where those transfers are repetitive or systematic, if that is necessary to achieve the public interest at issue.

(41) Regulation (EU) 2018/1725 of the European Parliament and of the Council[16] 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[17] applies to**~~

---

[16] 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).

[17] ~~**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,**~~

~~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 (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.

~~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).~~

(44) The storing of **information**~~personal data~~, or the gaining of access to **information**~~personal data~~ already stored, in a terminal equipment and the subsequent processing of such data should be regulated under a single legal framework, namely **Directive 2002/58/EC on privacy and electronic communications**~~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 **to this Directive should**~~presented in this Regulation~~ 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~~**Privacy enhancing technologies that reduce the processing of personal data** ~~relevant rules should also apply regardless of whether the terminal~~**and** ~~equipment~~**support** ~~is~~**the** ~~owned~~**effective** ~~by~~**implementation of** the ~~natural~~**obligations** ~~person~~**of** ~~or~~**data minimisation and data protection** by **design** ~~lanotheregalornatural~~ **and by default** ~~person~~**under Regulation (EU) 2016/679 can play a crucial role in maintaining citizens' trust in online digital ecosystems and it is important to incentivise the update of such technologies**.

(44a) The storing of **information**~~personal data~~, or the gaining of access to **information**~~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.~~

(44b) 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 **a subscriber or user**~~the data subject~~, it is necessary to define a limitative list of purposes for which the processing should be permitted without consent. As regards storing of **information**~~personal data~~, or the gaining of access to **information**~~personal data~~ already

stored, in a terminal equipment, and subsequent processing that is necessary for those purposes, **the Directive**~~this Regulation~~ should therefore provide that **such**~~the~~ processing is lawful**, including when being carried out jointly with or on the behalf of a**~~. The~~ controller**. For example**~~, such as~~ a media service provider, may mandate a **third party**~~processor~~, such as a market research company, to carry out **such**~~the~~ processing**.** ~~on its behalf.~~

(44c) Consent should not be required, where placing of information on or gaining access to information stored is necessary to provide a service explicitly requested by user or subscriber. This should include placing of information or gaining access to information stored for the purpose of ensuring certain functionalities necessary for the service explicitly requested by the user or subscriber. This could include memorising the user's choices and selected elements such as, among others, the user's language settings, configuration choices, items placed in shopping baskets, information to facilitate filling in of online forms, or functionalities of a requested service related to information on vehicles.

(44d) In order to improve their services, providers of online services should be able to gain information about the use of their service on an aggregated level without analysing individual subscriber or user behaviour. To enable this, measuring the audience of an online service by creating anonymous aggregated information about the usage of an online service, where it is carried out by the provider of that online service, or by a provider acting on their behalf should not require consent. The aggregated data used for such measurement should not relate to a specific data subject and should therefore be anonymous. Data of users or subscribers used for this purpose should not be further processed for another purpose nor 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. The aggregated information could be shared with third parties, including companies and non-commercial organizations. ~~In addition, Regulation (EU) 2024/1083 emphasises the importance of audience measurement for evaluating the performance of media content and understanding the preferences of audiences in order to plan the future production of content, as well as for its important function in fostering transparency and verifiability of audiences. Such measurement should be in principle carried out in accordance with widely accepted industry self-regulatory mechanisms, such as joint industry committees, and is often~~

~~conducted by independent entities acting as joint controllers. Thus, measuring audiences of media content by collecting data about the number and characteristics of viewers of the media content on the website of the provider or on online platforms should be possible without consent, provided that data collected are not further processed for another purpose, are immediately pseudonymised and that audience measurement reports generated do not contain personal data. Exempting such measurement from the consent requirement should contribute to the sustainability of the media ecosystem as highlighted in Regulation 2024/1083. The limitations should ensure that the personal data collected is not reused for providing personalised advertising, profiling or other unrelated purposes~~

(44e) Regulation (EU) 2024/1083 emphasises the importance of audience measurement for evaluating the performance of media content and understanding the preferences of audiences in order to plan the future production of content and for the purposes of decisions regarding advertising allocation and pricing, as well as for fostering transparency and verifiability of audiences. Such measurement should be in principle carried out in accordance with widely accepted industry self-regulatory mechanisms, such as joint industry committees, and is often conducted by independent entities acting as joint controllers under Regulation (EU) 2016/678. Thus, measuring audiences of media services or of content on online platforms by collecting data about the number and characteristics of users of media services or users of content on online platforms should be possible without consent, provided that data collected are not processed for another purpose, are pseudonymised and that audience measurement reports generated do not contain personal data. Exempting such measurement from the consent requirement should contribute to the sustainability of the media ecosystem as highlighted in Regulation 2024/1083. The limitations should ensure that the personal data collected is not reused for providing personalised advertising, profiling or other unrelated purposes. The reports containing anonymous and aggregated information could be shared with third parties, including companies and non-commercial organisations.

(~~44e~~44f) 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~~,~~ and proportionate, ~~discretely packaged and do not in any way change the functionality~~to maintain or restore the

security of the ~~software on the~~**service or** terminal equipment, ~~including the interaction~~**are provided separately from functionality updates where technically feasible, and do not introduce changes to functionality, interactions** 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~~ **beyond what is strictly necessary and proportionate for that security purpose.** ~~the~~**The** subscriber or user has the possibility to turn off the automatic installation of these updates. The maintaining or restoring the security of the service or of the terminal equipment should include in particular cybersecurity and the necessary security requirements to ensure a proper functioning of the terminal equipment as well as the protection of personal data and privacy of the user.

(~~44f~~**44g)** ~~Although the~~**The** simple display of contextual advertising does not typically require access to or storing of information on a user or subscriber**'s** device**. Contextual advertising is placed solely on the basis of the immediate content displayed on the subscriber or user's online interface – such as a website or an app - during an individual visit or on the basis of a single search query. Such advertising does not involve the processing of personal data, and it is not based on profiling, and it does not involve retention or link with an individual's past of future activity. At the same time, the effectiveness of** such advertising often relies on the possibility to measure the **display and the** performance of ~~advertising campaigns (~~**the advertisement displayed** such as capping cookies~~,~~ **and** advertising ~~audience~~ **measurement cookies**~~, or cookies to combat click fraud)~~**. Such measurement of the display and performance of contextual** advertising ~~which is made solely on the basis of the immediate content displayed on the user's interface may~~**should** be lawful without the consent of the user ~~provided~~**where** it is ~~not based on any type of profiling, in other words based on a user's visit to a single web page~~**carried out by the provider of an online service, including jointly with others,** or on ~~a single search query~~**behalf of that provider,** ~~and~~ provided ~~it~~**that data collected are pseudonymised after collection, as a key security measure, and are not processed for another purpose including profiling or providing programmatic advertising, and that the measurement** does not involve any **profiling nor processing of data relating to the subscriber or user'**~~data retention or link with the user's~~ **past or future activity, including activity across sites, apps or services.**

(44g) For the **further**~~subsequent~~ 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 **further**~~subsequent~~ 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) **Subscribers or users**~~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 **provider**~~controller~~'s online service again. This may have detrimental effects to the **subscribers or users**~~data subjects~~ which may consent just in order to avoid repeating requests. The **provider**~~controller~~ should therefore be obliged to respect the **subscriber or users'**~~data subject's~~ choices to refuse a request for consent for at least a certain period. **This obligation is applicable to any provider that accesses or stores information in the terminal equipment of a subscriber or user, including so-called third-party cookie.**

~~(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.~~

~~(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 **establishment by Member States of a national entry**~~single-entry~~ point ~~for incident reporting~~ should **support and facilitate the fulfilment of**~~allow entities to fulfil reporting~~ obligations **to the reporting of incidents and related events** 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 **national entry**~~single-entry~~ point **could**~~should~~ give a possibility for entities to retrieve information that they have previously submitted using the ~~single-entry~~**national 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 an incident reporting information point for incident reporting. That information point should serve as a clearly arranged source of information to support entities in identifying their reporting obligations and to guide them to the appropriate national entry point. Further information on related obligations, especially in terms of cybersecurity risk management, may be added. 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 **national entry points in particular and with a view to designing interoperable national entry points**~~the single-entry point~~, ENISA should **develop non-binding recommendations addressing the**~~take~~ appropriate and proportionate technical, operational and organisational measures **for Member States to develop, maintain and securely operate their respective national entry**~~to manage the risks posed to the security of the single-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 **establish a cross-sector working group to develop these recommendations in cooperation with CSIRTs and**~~consult~~ competent authorities under the relevant Union legal acts**, making use of existing cooperation groups and networks of Member States established under these acts, with a view draft** ~~when drafting~~ the technical, operational and organisational measures necessary to establish, maintain and securely operate the **national entry**~~single 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 an online digital interface, platform or technical interoperability hub, established and maintained by the Member State, supporting entities to fulfil their incident notification obligations across multiple regulatory frameworks through notifications at national level which will reach all competent authorities, CSIRTs and/or other designated 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 CSIRT's and competent and/or other designated 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, CSIRT's and/or other designated authorities within each national system.

(50b) The national entry point could, depending on Member States' organisational arrangement and national structure, allow for tasks and functionalities supporting the reporting of relevant incidents, such as enabling the submission of notifications, receiving and processing notifications submitted by entities, ensuring or facilitating access to such notifications for the competent authorities under the relevant Union act, transmitting or making available relevant information to other national authorities, where foreseen under Union or national law, supporting coordination among competent authorities in relation to reported incidents or information, or providing guidance or assistance to entities regarding notification procedures.

(~~50b~~50c) **The development and operation of national entry points may involve important costs for Member States, particularly where national reporting systems need to be built or existing ones need to be adapted. Further costs might be related to ensuring their cross-border interoperability. It is therefore 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) **It is important to support the further harmonisation of incident**~~Before enabling the~~ 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 **exchange and interoperability of information regarding incident reporting. For this purpose and in cooperation withhe**~~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~~ CSIRTs network**, the Cooperation Group and** ~~and the~~ 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 **develop guidelines to foster the harmonisation of incident notifications**~~take all necessary corrective measures, followed by a reassessment by the Commission~~.

~~(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~~

PUBLIC

~~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 **national entry**~~single-entry~~ point, while ensuring continuity and stability of the existing reporting framework~~, and considering that the~~ national entry~~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 **national entry**~~single-entry~~ point under Directive (EU) 2022/2555, Directive (EU) 2022/2557 or Regulation (EU) 2016/679, where appropriate. For this purpose, **Member States**~~the Commission~~ should take due account of the regulatory technical standards adopted pursuant to Regulation (EU) 2022/2554 **and the reporting templates developed under Directive (EU) 2022/2555 (NIS2)**, which specify the content of the initial notification, as well as the intermediate and final reports, concerning major ICT-related incidents. **While appropriate sector-specific adaptation should remain possible,** ~~This~~ **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 national entry~~**single-entry point should be designed to accommodate and support the exchange of information at that level for each relevant Union legal act, ensuring it is important to ensure** that appropriate data flows between authorities are enabled in a secure, timely, and efficient manner, **while remaining under the control of Member States,** should the Member States decide to make use of this additional feature.

(56) To ensure that incident reporting is carried out via the **national entry**~~single-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 **national entry**~~single-entry~~ point should start being used for the purpose of reporting under those acts within **30**~~18~~ months from the entry into force of this Regulation. **Any new amendment to other Union legal acts or new proposals for Union legal acts should establish**~~When the Commission initiates the mechanisms of the notice delaying~~ the date **when national**~~of application to 24 months from the~~ entry **point**~~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 **be used for**~~continue to apply for the purpose of meeting the~~ reporting **incidents or related events.** ~~obligations laid down in the provisions.~~

(57) In the exceptional event that a technical impossibility prevents the submission of incident notifications using the **national entry**~~single-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 **and the European Data Protection Board were**~~was~~ consulted in accordance with Article **42**~~42(1)~~ of Regulation (EU) 2018/1725 of the European Parliament and of the Council[18], and delivered **their joint**~~its~~ opinion on **10**

[18] 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

February 2026~~[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]~~.

(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) **2019/1150**~~2019/1050~~ should be **deleted**~~repealed~~. Regulation (EU) 2022/2065 and Regulation (EU) 2022/1925 contribute to a fully harmonised regulatory framework for 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, **on ranking in Article 5, and on differentiated treatment in Article 7,**~~as well as~~ on the internal complaint-handling system in Article 11**, as well as provisions in**~~ 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~~ Article 15 ensuring enforcement~~, will temporarily remain in application until the original acts are amended~~ **and in Article 18(1) mandating the Commission to evaluate that Regulation 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

---

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).

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.

(62) The reasons that led the European Parliament and the Council to adopt those provisions of Regulation (EU) 2022/868, Regulation (EU) 2018/1807, and Directive 2019/1024 which are being re-enacted in the present regulation remain valid.

HAVE ADOPTED THIS REGULATION:

Article 1

Amendments to Regulation (EU) 2023/2854

Regulation (EU) 2023/2854 is amended as follows:

1. Article 1 is amended as follows:

(-a) in paragraph 1 point (c) is replaced by the following:
'(c) the making available of data by data holders to public sector bodies, the Commission, the European Central Bank and Union bodies, where there is the need for those data for the performance of a specific task carried out in the public interest;'

(a) in paragraph 1, the following points are inserted:

'(ea) voluntary registration of data intermediation services;

(eb) voluntary registration of entities which collect and process data made available for altruistic purposes;

(ec) the establishment of a European Data Innovation Board;

(ed) data localisation requirements ~~and the availability of data to competent authorities;~~

(ee) the re-use of certain data and documents held by public sector bodies or by certain public undertakings, and of research data.;

(aa) in paragraph 2, point (f) is replaced by the following:

'(f) Chapter VII applies to any non-personal data held in the Union by providers of data processing services, public sector bodies making available data in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data in accordance with Chapter VIIc Section 3 was granted, a data intermediation services provider or a recognised data altruism organisation.'. '

(b) in paragraph 2, the following points are added:

~~'(g) Chapter VIIa applies to personal and non-personal data;~~

(h) Chapter VIIb applies to any non-personal data;

~~(i) Chapter VIIc applies to personal and non-personal data, namely the following:~~

~~(i) documents held by public sector bodies of Member States as referred~~

~~(1) to in Article 32i(1), point (a) or by public undertakings as referred~~

~~(2) to in Article 32i(1), point (b);~~

~~(ii) research data as referred to in Article 32i(1), point (c);~~

~~(iii) certain categories of protected data as referred to in Article 32i(1), point (a).'~~

(c) in paragraph 3, **points (e) and (g) are**~~point (g) is~~ replaced by the following:

~~(ca)~~ **'(e) public sector bodies, the Commission, the European Central Bank and Union bodies that request data holders to make data available where there is the need for those data for the performance of a specific task carried out in the**

public interest and to the data holders that provide those data in response to such request;

‘(g) participants in data spaces.;

(ca) in paragraph (5) the following subparagraph is added:

~~gb~~ **‘The rules set out in Chapters VIIa and VIIc do not create a legal basis for the processing of personal data.’’**

(d) paragraph 7 is deleted.

(e) the following paragraphs 11, 12 and 13 are added:

‘11. Chapter VIIb of this Regulation is without prejudice to laws, regulations, and administrative provisions that relate to the internal organisation of Member States and that allocate, among public authorities and bodies governed by public law, powers and responsibilities for the processing of data without contractual remuneration of private parties, as well as to laws, regulations, and administrative provisions of Member States that provide for the implementation of such powers and responsibilities.

12. Where sector-specific Union or national law requires public sector bodies, data intermediation services providers or recognised data altruism organisations to comply with specific additional technical, administrative or organisational requirements that relate to Chapters VIIa and VIIb, including through an authorisation or certification regime, those provisions of that sector-specific Union or national law shall also apply. Any such specific additional requirements shall be non-discriminatory, proportionate and objectively justified.’

13. With regards to data and documents in scope of Section II of Chapter VIIc, Chapter VIIc of this Regulation **establishes a set of minimum rules governing the re-use and the practical arrangements for facilitating the re-use of data and documents and** does not affect the possibility for Member States to adopt more detailed or stricter rules, provided that those rules allow for more extensive re-use of data and documents.’’

PUBLIC

2. Article 2 is amended as follows:

(a) the following points (4a), (4b) and (4c) are inserted:

'(4a) 'consent' means consent as defined in Article 4, point (11), of Regulation (EU) 2016/679;

(4b) 'permission' **in the context of Chapters VIIa and VIIc** means giving data users the right to the processing of non-personal data;

~~(4c) 'access' means data use, in accordance with specific technical, legal or organisational requirements, without necessarily implying the transmission or downloading of data;~~

(b) point (10) is replaced by the following:

~~4cb.~~ **'(10) 'data intermediation service' means a service which aims to establish relationships of an economic character for the purposes of data sharing between an undetermined number of data subjects or data holders and data users, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data, and which :**

~~4cc.~~ **(a) does not have as its main purpose the intermediation of copyright-protected content;**

~~4cd.~~ **(b) is not jointly procured by several legal persons for exclusive use among them; '**

(b) point (13) is replaced by the following:

'(13) 'data holder' means a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use or make available data, including, where contractually agreed, product data or related service data, which it has retrieved or generated during the provision of a related service;'

PUBLIC

(ba) point (28) is replaced by the following:

'(28) 'public sector body' means the State, national, regional or local authorities of the Member States and bodies governed by public law of the Member States, or associations formed by one or more such authorities or one or more such bodies.

(c) the following points (28a) and (28b) are inserted:

'(28a) 'bodies governed by public law' means bodies that have all of the following characteristics:

(a) they are established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character;

(b) they have legal personality;

(c) they are financed, for the most part by the State**, national**, regional or local authorities, or by other bodies governed by public law; or are subject to management supervision by those authorities or bodies; or have an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, **national,** regional or local authorities, or by other bodies governed by public law;

(28b) 'public undertaking' means any undertaking over which a public sector body may exercise directly or indirectly a dominant influence by virtue of their ownership of it, their financial participation therein, or the rules which govern it. A dominant influence on the part of the public sector bodies shall be presumed in any of the following cases in which those bodies, directly or indirectly:

(a) hold the majority of the undertaking's subscribed capital;

(b) control the majority of the votes attaching to shares issued by the undertaking;

(c) can appoint more than half of the undertaking's administrative, management or supervisory body;;'

PUBLIC

(e)~~(d)~~the following **point (38a) is**~~points (38a) and (38b) are~~ inserted:

~~'(38a) 'data intermediation service' means a service which aims to establish relationships of an economic character for the purposes of data sharing between an undetermined number of data subjects or data holders and data users, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data, and which:~~

~~(1) do not have as their main purpose the intermediation of copyright-protected content;~~

~~(2) are not jointly procured by several legal persons for exclusive use among them;~~

(**38a**~~38b~~) 'data altruism' means the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or of permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest;

(ea) point (39) is deleted.

(f) point (42) is amended as follows:

~~38bc.~~ **(42) 'common specifications' means a set of technical requirements, other than a standard, that provides means of complying with certain requirements and obligations established under this Regulation.'**

(e) the following points (44) to (**62**~~63~~) are added:

'(44) 'medium-sized enterprise' means a medium-sized enterprise as defined in **point**~~Article~~ 2 of Annex I to Recommendation 2003/361/EC;

PUBLIC

(45) ‘small mid-cap’ or ‘SMC’ means a small mid-cap enterprise as defined in **point**~~Article~~ 2 of the Annex to Commission Recommendation (EU) 2025/1099;

(46) ‘university’ means **any**~~a~~ public sector body that provides post-secondary-school higher education leading to academic degrees;

(47) ‘standard licence’ means a set of predefined re-use conditions in a digital format, preferably compatible with standardised public licences available online;

(48) ‘document’ means:

(a) any content that is non-digital whatever its medium (paper or as a sound, visual or audiovisual recording); or

(b) any part of such content;

(49) ‘dynamic data’ **in the context of Chapter VIIc** means data ~~and documents in a digital form~~, subject to frequent or real-time updates, in particular because of their volatility or rapid obsolescence; data generated by sensors are typically considered to be dynamic data;

(50) ‘research data’ means data~~,~~, other than scientific publications, which are collected or produced in the course of scientific research activities and are used as evidence in the research process, or are commonly accepted in the research community as necessary to validate research findings **or**~~and~~ results;

(51) ‘re-use’ means the use by natural ~~persons~~ or legal **persons of data or**~~entities of~~ documents held by:

(a) public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the **data or** documents were produced, except for the exchange of **data or** documents between public sector bodies purely in pursuit of their public tasks; or

(b) public undertakings, under Chapter VIIc Section 2 for commercial or non-commercial purposes other than for the initial purpose of providing

PUBLIC

services in the general interest for which the **data or** documents were produced, except for the exchange of **data or** documents between public undertakings and public sector bodies purely in pursuit of the public tasks of public sector bodies;

(52) 'high-value datasets' means data and documents the re-use of which is associated with important benefits for society, the environment and the economy, in particular because of their suitability for the creation of value-added services, applications and new, high-quality and decent jobs, and because of the number of potential beneficiaries of the value-added services and applications based on those data and documents;

(53) 'certain categories of protected data' means data ~~and documents~~ held by public sector bodies which are protected on the grounds of

(a) commercial confidentiality, including business, professional and company secrets;

(b) statistical confidentiality;

(c) the protection of intellectual property rights of third parties; or

(d) the protection of personal data, insofar as such data fall outside the scope of Section 2 of Chapter VIIc;

(54) 'secure processing environment' means the physical or virtual environment and organisational means to ensure compliance with Union law in particular with regard to data subjects' rights, intellectual property rights, and commercial and statistical confidentiality, integrity and accessibility, as well as with applicable national law, and to allow the entity providing the secure processing environment to determine and supervise all data processing actions, including the display, storage, download and export of data and the calculation of derivative data through computational algorithms;

(55) 're-user' means a natural or legal person who was granted the right to re-use data or documents held by a public sector body or a public undertaking under Chapter VIIc or to research data or certain categories of protected data;

(56) ‘machine-readable format’ means a file format structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure;

(57) ‘open format’ means a ~~file~~ format that is platform-independent and made available to the public without any restriction that impedes the re-use of **data** ~~documents~~;

(58) ‘formal open standard’ means a standard which has been laid down in written form, detailing specifications for the requirements on how to ensure software interoperability;

(59) ‘reasonable return on investment’ means a percentage of the overall charge, in addition to the amount needed to recover the eligible costs, not exceeding 5 percentage points above the fixed interest rate of the ECB;

(60) ‘data localisation requirement’ means any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law, including in the field of public procurement, without prejudice to Directive 2014/24/EU, which imposes the processing of data in the territory of a specific Member State or hinders the processing of data in any other Member State;

(61) ‘draft act’ means a text drafted for the purpose of being enacted as a law, regulation or administrative provision of a general nature, the text being at the stage of preparation at which substantive amendments can still be made;

(**62**~~61~~) ‘pseudonymisation’ means pseudonymisation as referred to under Article 4(5) of Regulation (EU) 2016/679.’

3. in Article 4, paragraph 8 is replaced by the following:

‘8. ~~In exceptional circumstances,~~ **Where**~~where~~ the data holder who is a trade secret holder is able to demonstrate that~~, despite the technical and organisational~~

~~measures taken by the user pursuant to paragraph 6 of this Article,~~ it is ~~highly~~ likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the user poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse ~~on a case-by-case basis~~ a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to the user without undue delay. ~~Where the data holder refuses~~

Data holders who refuse to share data pursuant to ~~this paragraph, it~~**the first sub-paragraph** shall notify **all instances of refusal to** the competent authority designated pursuant to Article 37~~.~~ **every 3 months.**

The Commission shall issue guidelines, in consultation with the European Data Innovation Board (EDIB), on the application of this paragraph, such as the assessment of serious economic damage, and the enforceability of trade secrets protection in third countries.~~;~~**'**

4. in Article 5, paragraph 11 is replaced by the following:

'11. ~~In exceptional circumstances,~~ **Where**~~where~~ the data holder who is a trade secret holder is able to demonstrate that~~, despite the technical and organisational measures taken by the third party pursuant to paragraph 9 of this Article,~~ it is ~~highly~~ likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the third party poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law, that data holder may refuse ~~on a case-by-case basis~~ a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to

the third party without undue delay. ~~Where the data holder refuses~~

Data holders who refuse to share data pursuant to ~~this paragraph, it~~**the first sub-paragraph** shall notify **all instances of refusal to** the competent authority designated pursuant to Article 37~~.~~ **every 3 months.**

The Commission shall issue guidelines, in consultation with the European Data Innovation Board (EDIB), on the application of this paragraph, such as the assessment of serious economic damage, and the enforceability of trade secrets protection in third countries.'~~;~~

4a- In article 10 paragraph 12 is replaced by the following:

~~11b.~~ **'(12) The decision of a dispute settlement body shall be binding on the parties only if the parties have explicitly agreed to its binding nature prior to the start of the dispute settlement proceedings'.**

4a. in Article 11 paragraph 1 is replaced by the following:

~~11b.~~ **'(1) A data holder may apply appropriate technical protection measures, including encryption, to prevent unauthorised access to data, including metadata, and to ensure compliance with Articles 4, 5, 6, 8 and 9, as well as with the agreed contractual terms for making data available. Such technical protection measures shall not discriminate between data recipients or hinder a user's right to obtain a copy of, retrieve, use or access data, to provide data to third parties pursuant to Article 5 or any right of a third party under Union law or national legislation adopted in accordance with Union law. Users, third parties and data recipients shall not alter or remove such technical protection measures unless agreed by the data holder.'**

5. the title of Chapter V is replaced by the following:

'MAKING DATA AVAILABLE TO PUBLIC SECTOR BODIES, THE COMMISSION, THE EUROPEAN CENTRAL BANK AND UNION BODIES ON THE BASIS OF A PUBLIC EMERGENCY;'

6. Articles 14 and 15 are deleted;

7. the following Article 15a is inserted:

‘Article 15a

Obligation for data holders to make data available on the basis of a public emergency

1. Where a public sector body, the Commission, the European Central Bank or a Union body demonstrates **the**~~an exceptional~~ need to use certain data to carry out its statutory duties in the public interest when responding to, ~~ mitigating,~~ or supporting the recovery from a public emergency, it may request from data holders that are legal persons, other than public sectors bodies, to make available those data, including the metadata necessary to interpret and use those data. Upon such duly reasoned request, data holders shall make the data and metadata available to the requesting public sector body, the Commission, the European Central Bank or Union body. Such requests may also be made where the production of official statistics is required in relation to a public emergency.

2. Where the data requested are necessary to respond to a public emergency, and the requesting body pursuant to paragraph 1 is unable to obtain such data by other means in a timely and effective manner under equivalent conditions, the request shall concern non-personal data. Where the provision of non-personal data is insufficient to **respond to**~~address~~ the public emergency, personal data may also be requested and, ~~where possible~~, made available in **pseudonymised**~~pseudonymized~~ form, subject to appropriate technical and organisational measures to ensure their protection.

3. Where the data requested are necessary to ~~mitigate or~~ support the recovery from a public emergency **and the**~~, a~~ requesting body pursuant to paragraph 1 acting on the basis of Union or national law **is unable to obtain such data by other means in a timely and effective manner under equivalent conditions**, **it** may request specific non-personal data, the lack of which **prevents**~~prevent~~ it from ~~mitigating or~~ supporting the recovery from a public emergency. Such requests shall not be made to microenterprises and small enterprises.;**’’**

8. in Article 16, paragraph 2 is replaced by the following:

‘2. This Chapter shall not apply to activities carried out by public sector bodies, the Commission, the European Central Bank or Union bodies relating to the prevention,

investigation, detection or prosecution of criminal or administrative offences or the execution of criminal penalties, or to customs or taxation administration. This Chapter does not affect Union or national law governing such activities.'

9. Article 17 is amended as follows:

(a) paragraph 1 is amended as follows:

(i) the introductory wording is replaced by the following:

'When requesting data pursuant to Article 15a, a public sector body, the Commission, the European Central Bank or a Union body shall:;'

(ii) points (b) and (c) are replaced by the following:

'(b) demonstrate that the conditions **for the** ~~**to make a**~~ request under Article 15a are met;

(c) explain the purpose of the request, the intended use of the data requested, including, where applicable, by a third party in accordance with paragraph 4 of this Article, the duration of that use, and, where relevant, how the processing of personal data is to address the public emergency;;'

(b) paragraph 2 is amended as follows:

(i) point (c) is replaced by the following:

'(c) be proportionate to the public emergency and duly justified, regarding the granularity and volume of the data requested and the frequency of access to the data requested;;'

(ii) point (e) is deleted.;

(iii) Point (i) is replaced by the following:

~~(iii)~~ **'(i)where personal data are requested, be notified without undue delay to the supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679 in the Member State where the public sector**

body is established or to the EDPS where the request is made by the Commission, the European Central Bank or a Union body.'

(ba) paragraph 4 is replaced by the following:

~~(iid)~~ **'Paragraph 3 of this Article does not preclude a public sector body, the Commission, the European Central Bank or a Union body to exchange data obtained pursuant to this Chapter with another public sector body or the Commission, the European Central Bank or a Union body in view of completing the tasks referred to in Article 15a, as specified in the request in accordance with paragraph 1, point (f), of this Article or to make the data available to a third party where it has delegated, by means of a publicly available agreement, technical inspections or other functions to that third party. The obligations on public sector bodies pursuant to Article 19, in particular safeguards to preserve the confidentiality of trade secrets, shall apply also to such third parties. Where a public sector body, the Commission, the European Central Bank or a Union body transmits or makes data available under this paragraph, it shall notify the data holder from whom the data was received without undue delay.'**

(c) paragraphs 5 and 6 are deleted;

10. Article 18 is amended as follows:

(a) in paragraph 2, the introductory wording is replaced by the following:

'2. Without prejudice to specific needs regarding the availability of data defined in Union or national law, a data holder may decline or seek the modification of a request to make data available under this Chapter without undue delay and, in any event, no later than five working days after the receipt of a request pursuant to Article 15a(2) and without undue delay and, in any event, no later than 30 working days after the receipt of a request pursuant to Article 15a(3), on any of the following grounds:;'

(b) paragraph 5 is deleted;

11. Article 19 is amended as follows:

(a) in paragraph 1, the introductory wording is replaced by the following:

'A public sector body, the Commission, the European Central Bank or a Union body receiving data pursuant to a request made under Article 15a shall:;'

(aa) point (c) of paragraph 1 is replaced by the following:

~~(ab)~~ **c) erase the data as soon as they are no longer necessary for the stated purpose and inform the data holder and individuals or organisations that received the data pursuant to Article 21(1) without undue delay that the data have been erased, unless archiving of the data is required in accordance with Union or national law on public access to information in the context of transparency obligations.'**

(b) paragraph 3 is replaced by the following:

'3. Disclosure of trade secrets to a public sector body, the Commission, the European Central Bank or a Union body shall be required only to the extent that it is strictly necessary to achieve the purpose of a request under Article 15a. In such a case, the data holder or, where they are not the same person, the trade secret holder shall identify the data which are protected as trade secrets, including in the relevant metadata. The public sector body, the Commission, the European Central Bank or the Union body shall, prior to the disclosure of trade secrets, take all necessary and appropriate technical and organisational measures to preserve the confidentiality of the trade secrets, including, as appropriate, the use of model contractual terms, technical standards and the application of codes of conduct.;'

12. Article 20 is replaced by the following:

'Article 20

Compensation for making data available under Chapter V

1. Data holders shall make available data necessary to respond to a public emergency pursuant to Article 15a(2) free of charge. The public sector body, the Commission, the European Central Bank or the Union body that has received data shall provide public acknowledgement to the data holder if requested by the data holder.

2. The data holder shall be entitled to fair compensation for making data available in compliance with a request made pursuant to Article 15a(3). Such compensation shall cover the technical and organisational costs incurred to comply with the request including, where applicable, the costs of anonymisation, pseudonymisation, aggregation and of technical adaptation, and a reasonable margin. Upon request of the public sector body, the Commission, the European Central Bank or the Union body, the data holder shall provide information on the basis for the calculation of the costs and the reasonable margin.

3. By way of derogation from paragraph 1 of this Article, a data holder that is a microenterprise or small enterprise may claim compensation for making data available in response to a request under Article 15a(2), according to the conditions set in paragraph 2 of this Article.

4. Data holders shall not be entitled to compensation for making data available in compliance with a request made pursuant to Article 15a**(2) or 15a**(3), where the **statutory duty**~~specific task~~ carried out in the public interest is the production of official statistics and where the purchase of data is not allowed by national law. Member States shall notify the Commission where the purchase of data for the production of official statistics is not allowed by national law.**'**;'

13. Article 21 is amended as follows:

(a) the heading is replaced by the following:

'Sharing of data obtained in the context of a public emergency with research organisations or statistical bodies;'

(b) paragraph 5 is replaced by the following:

'5. Where a public sector body, the Commission, the European Central Bank or a Union body intends to transmit or make data available under paragraph 1, it shall without undue delay notify the data holder from whom the data was received, stating the following:

(a) the identity and contact details of the organisation or the individual receiving the data;

(b) the purpose of the transmission or making available of the data;

(c) the period for which the data is to be used ~~and the technical protection~~;

(d) the **technical protection and** organisational measures taken, including where personal data or trade secrets are involved.;'

14. The following Article 22a is inserted before Chapter VI:

'Article 22a

Right to lodge a complaint

Where a dispute arises concerning a request for data under Article 15a, including its refusal, modification, the level of compensation, or the transmission or making available of data, the data holder, the public sector body, the Commission, the European Central Bank or the Union body may lodge a complaint with the competent authority, designated pursuant to Article 37, of the Member State where the data holder is established.;'

15. in Article 31, the following paragraphs 1a**, 1b, and 1c** ~~and 1b~~ are inserted:

'1a. The obligations laid down in Chapter VI, with the exception of Article 29, and in Article 34 shall not apply to data processing services other than those referred to in Article 30(1), where the majority of features and functionalities of the data processing service has been adapted by the provider to the specific needs of the customer, if the provision of such services is based on a contract concluded before or on 12 September 2025.

The provider of such data processing services shall not be required to renegotiate or amend a contract for the provision of those services before its expiry if that contract was concluded before or on 12 September 2025. Any contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.

~~1b. A provider of a data processing service may include provisions on proportionate early termination penalties in a contract of fixed duration on the provision of data processing services other than those referred to in Article 30(1).~~

1b. Where the provider of data processing service is a small and medium-sized enterprise or a small mid-cap, the obligations laid down in Chapter VI, with the exception of Article 29, and in Article 34 shall not apply to data processing services other than those referred to in Article 30(1), if the provision of such services is based on a contract concluded before or on 12 September 2025.

Where the provider of a data processing service is a small and medium-sized enterprise or a small mid-cap, the provider shall not be required to renegotiate or amend a contract for the provision of a data processing service other than those referred to in Article 30(1) before its expiry 1 if that contract was concluded before or on 12 September 2025. Any contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.~~;~~

1c. A provider of a data processing service may include provisions on proportionate early termination penalties in a contract of fixed duration on the provision of data processing services.';'

16. Article 32 is amended as follows:

(a) paragraph 1 and 2 are replaced by the following:

'1. Providers of data processing services, the public sector body making available data ~~or documents~~ in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data ~~or documents~~ in accordance with Chapter VIIc Section 3 was granted, a data intermediation services provider or a recognised data altruism organisation shall take all adequate technical, organisational and legal measures, including contracts, in order to prevent international and third-country governmental access and transfer of non-personal data held in the Union where such transfer or access would create a conflict with Union law or with the national law of the relevant Member State, **including criminal law provisions of Member States, or national law provisions protecting their essential security interests within the meaning of Article 4(2) of the Treaty on European Union,** without prejudice to paragraph 2 or 3.

2. Any decision or judgment of a third-country court or tribunal and any decision of a third-country administrative authority requiring a provider of data processing services, the public sector body making available data ~~or documents~~ in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data ~~or documents~~ in accordance with Chapter VIIc Section 3 was granted, a data intermediation services provider or a recognised data altruism organisation to transfer or give access to non-personal data falling within the scope of this Regulation held in the Union shall be recognised or enforceable in any manner only if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union, or any such agreement between the requesting third country and a Member State.;'

(b) in paragraph 3, first subparagraph, the introductory wording is replaced by the following:

'3. In the absence of an international agreement as referred to in paragraph 2, where a provider of data processing services, the public sector body making available data ~~or documents~~ in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data ~~or documents~~ in accordance with Chapter VIIc Section 3 was granted, a data intermediation services provider or a recognised data altruism organisation is the addressee of a decision or judgment of a third-country court or tribunal or a decision of a third-country administrative authority to transfer or give access to non-personal data falling within the scope of this Regulation held in the Union and compliance with such a decision or judgement would risk putting the addressee in conflict with Union law or with the national law of the relevant Member State, transfer to or access to such data by that third-country authority shall take place only where:';'

(c) paragraphs 4 and 5 are replaced by the following:

'4. If the conditions laid down in paragraph 2 or 3 are met, the provider of data processing services, the public sector body making available data ~~or documents~~ in accordance with Chapter VIIc Section 3, the natural or legal

person to which the right to re-use data ~~or documents~~ in accordance with Chapter VIIc Section 3 was granted, the data intermediation services provider or the recognised data altruism organisation shall provide the minimum amount of data permissible in response to a request, on the basis of the reasonable interpretation of that request by the provider or relevant national body or authority referred to in paragraph 3, second subparagraph.

5. The provider of data processing services, the public sector body making available data ~~or documents~~ in accordance with Chapter VIIc Section 3, the natural or legal person to which the right to re-use data ~~or documents~~ in accordance with Chapter VIIc Section 3 was granted, the data intermediation services provider or the recognised data altruism organisation shall inform the natural or legal person whose rights and interests might be affected about the existence of a request of a third-country authority to access its data before complying with that request, except where the request serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity.;'

17. Article 36 is deleted.

18. the following Chapters VIIa, VIIb and VIIc are inserted:

'CHAPTER VIIa

Voluntary registration of data intermediation services and data altruism organisations'

Article 32a

Public Union registers **for voluntary data intermediation services and data altruism organisations**

(1) The Commission shall keep and regularly update public Union registers of:

(a) recognised data intermediation services providers**;** and

(b) recognised data altruism organisations.

(2) Data intermediation services providers registered in the public Union register referred to in paragraph 1 point (a) may use the label 'data intermediation services provider recognised in the Union' in its written and spoken communication, as well as a common logo referred to in paragraph 4.

(3) Data altruism organisations registered in the public Union register referred to in paragraph 1 point (b) may use the label 'data altruism organisation recognised in the Union' in its written and spoken communication, as well as the common logo referred to in paragraph 4.

(4) In order to ensure that data intermediation services providers **recognised in the Union and data altruism organisations** recognised in the Union are easily identifiable throughout the Union, the Commission is empowered to adopt implementing acts establishing a design for the common logo. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 46(1a).

Article 32b

Competent authorities for the registration of data intermediation services providers and data altruism organisations

(1) Each Member State shall designate one or more competent authorities responsible for the application and enforcement of this Chapter in accordance with Article 37(1).

(2) The competent authorities shall be set up in a manner so that their independence from any recognised data intermediation services provider or recognised data altruism organisation is guaranteed.

Article 32c

General requirements for registration of recognised data intermediation services providers

In order to qualify for registration in the public Union register referred to in Article 32a paragraph 1 point (a), ~~a~~ data intermediation services **providers**~~provider~~ shall meet all of the following requirements:

(a) they do not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users;

(b) the data they collect with respect to any activity of a natural or legal person for the purpose of the provision of the data intermediation service, including the date, time and geolocation data, duration of activity and connections to other natural or legal persons established by the person who uses the data intermediation service, are used only for the development of that data intermediation service**, which may entail the use of data for the detection of fraud or for cybersecurity.**~~;~~

(c) where they offer additional tools and services to data holders**,** ~~or~~ data subjects **or data users** for the specific purpose of facilitating the exchange of data, such as temporary storage, curation, conversion, encryption, anonymisation and pseudonymisation **or other relevant privacy-enhancing technologies**, such tools and services are used only at the explicit request or approval of the data holder or data subject **or data user**;

(d) where data intermediation service providers ~~which are not micro and small sized enterprises~~ offer ~~value-added~~ services to their clients other than **data intermediation services and the additional tools and**~~the~~ services referred to in point (c), they fulfil the following conditions:

(i) **such other**~~the value-added~~ services are explicitly requested by the **data holder, data subject or data** user;

(ii) the data are not used for other purposes than performing the **requested**~~value-added~~ service;

(iii) the **data intermediation**~~value-added~~ services are offered through **an entity**~~a~~ functionally separate **from entities offering other services**~~entity~~;

(iv) the undertaking seeking to offer the **other**~~value-added~~ services is not designated as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925;

(v) the commercial terms, including pricing, for the provision of data intermediation services to a data holder or data user are not dependent upon whether the data holder or data user uses o**ther**~~value-added~~ services provided by the data intermediation services provider or by a related entity;

(e) the data intermediation services provider offering services to data subjects acts in the data subjects' best interest where it facilitates the exercise of their rights, in particular by informing and, where appropriate, advising data subjects in a concise, transparent, intelligible and easily accessible manner about intended data uses by data users and standard terms and conditions attached to such uses before data subjects give consent.

(f) the data intermediation services provider ensures that the procedure for access to its service is fair, transparent and non-discriminatory for both data subjects and data holders, as well as for data users, including with regard to prices and terms of service;

(g) the data intermediation services provider maintains a log record of the data intermediation activity;

(h) the data intermediation services provider takes necessary technical or organizational measures to ensure an appropriate level of security for the storage, processing and transmission of non-personal data.

~~(ed)~~ **Point (d)(iii), of the first sub-paragraph does not apply to micro and small sized enterprises.**

Article 32d

General requirements for registration of recognised data altruism organisations

In order to qualify for registration in the public Union register referred to in Art. 32a paragraph 1 point (b), a data altruism organisation shall meet all of the following requirements:

(a) they carry out data altruism activities;

(b) they are a legal person established pursuant to national law to meet objectives of general interest as provided for in national law, where applicable;

(c) they operate on a not-for-profit basis and are legally independent from any entity that operates on a for-profit basis;

(d) they carry out their data altruism activities through a structure that is functionally separate from their other activities.

Article 32e

Registration **in public Union register**

(1) Data intermediation services provider which meets the requirements set out in Article 32c may submit an application for registration in the public Union register of recognised data intermediation services providers to the competent authority referred to in Article 32b in the Member State in which they have their main establishment.

A data~~Data~~ altruism organisation which meets the requirements set out in Article 32d may submit an application for registration in the public Union register of recognised data altruism organisations to the competent authority referred to in Article 32b in the Member State in which they have their main establishment.

(2) Data intermediation services providers and data altruism organisations that have no main establishment in the Union shall designate a legal representative in one of the Member States. The legal representative shall be mandated to be addressed in addition to or instead of the data intermediation services provider or data altruism organisation by competent authorities**, data users** or data subjects and data holders. The legal representative shall cooperate with and comprehensively demonstrate to the competent authority, upon request, the actions taken and provisions put in place by the data intermediation services provider or the data altruism organisation to ensure compliance with this Regulation. **Article 37(11) and (12) do not apply to data intermediation services providers and data altruism organisations.**

The data intermediation services provider or data altruism organisation shall be deemed to be under the jurisdiction of the Member State in which the legal representative is located. The designation of a legal representative shall be without prejudice to any legal

actions which could be initiated against the data intermediation services provider or data altruism organisation.

(3) Competent authorities shall establish the necessary application forms.

(4) Where a data intermediation services provider has submitted all necessary information pursuant to paragraph 3 of this Article, and complies with the requirements set out in Article 32c, the competent authority shall, within 12 weeks after the receipt of the application for registration, take a decision on whether the provider complies with the criteria set out in Article 32c. Where the **competent authority requests the applicant to provide additional information necessary to assess compliance with Article 32c, the time limit shall be suspended until the competent authority has received that information. In duly justified cases, where the assessment of compliance requires additional time due to the complexity or novelty of the services, the competent authority may extend the time limit once by a maximum of 12 weeks and shall inform the applicant accordingly, stating reasons. Where the** provider complies with the criteria, the competent authority shall submit the relevant information to the Commission which shall register the providers in the public Union register as a recognised data intermediation services provider.

The first subparagraph shall also apply where a data altruism organisation has submitted all necessary information pursuant to paragraph **3**~~2~~, and complies with the registration requirements set out in Article 32d.

The registration in the public Union register shall be valid in all Member States.

(5) The competent authority may charge fees for the registration in accordance with national law. Such fees shall be proportionate and objective and be based on the administrative costs related to the monitoring of compliance. In the case of small-mid caps, small and medium-sized enterprises, and start-ups, the competent authority may charge a discounted fee or waive the fee.

(6) Registered entities shall notify **within a reasonable time** the competent authority of any subsequent changes to the information as provided during the application process or where they cease their data intermediation or data altruism activities in the Union.

(7) The competent authority shall without delay and by electronic means notify the Commission of any notification pursuant to paragraph 6. The Commission shall without undue delay update the public Union register.

Article 32f

Duties of recognised data altruism organisations

(1) Recognised data altruism organisations shall inform data subjects or data holders prior to any processing of their data in a clear and easily comprehensible manner of the following:

(a) the objectives of general interest and, if applicable, the specified, explicit and legitimate purpose for which personal data is to be processed, and for which it permits the processing of their data by a data user;

(b) the location of the processing and the objectives of general interest for which it permits any processing carried out in a third country, where the processing is carried out by the recognised data altruism organisation.

(2) Recognised data altruism organisations shall not use the data for other objectives than the objectives of general interest for which the data subject or data holder allows the processing. The recognised data altruism organisation shall not use misleading marketing practices to solicit the provision of data.

(3) Recognised data altruism organisations shall provide electronic means for obtaining consent from data subjects or permissions to process data made available by data holders as well as for their withdrawal.

(4) Recognised data altruism organisations shall, without delay, inform data holders in the event of any unauthorised transfer, access or use of the non-personal data that it has shared.

(5) Where recognised data altruism organisations facilitate data processing by third parties, including by providing tools for obtaining consent from data subjects or permissions to process data made available by data holders, they shall, where relevant, specify the third-country in which the data use is intended to take place.

Article 32g

Monitoring of compliance

(1) The competent authorities referred to in Article 32b shall~~, either on their own initiative or on a request by a natural or legal person, monitor and~~ supervise whether recognised data intermediation services providers and recognised data altruism organisations comply with the requirements laid down in this Chapter, including whether they continue to comply with the requirements for registration laid down therein. **Those competent authorities may also monitor and supervise the compliance of data intermediation services providers and recognised data altruism organisations, on the basis of a request by a natural or legal person.**

(2) The competent authorities shall have the power to request from recognised data intermediation services providers or recognised data altruism organisations, or their legal representative, all the information that is necessary to verify compliance with the requirements laid down in this Chapter. Any request for information shall be proportionate to the performance of the task and shall be reasoned.

(3) Where a competent authority finds that a recognised data intermediation services provider or a recognised data altruism organisation does not comply with one or more of the requirements laid down in this Chapter, it shall notify that entity, or its legal representative, of those findings and give it the opportunity to state its views, within 30 days of the receipt of the notification.

(4) The competent authority shall have the power to require the cessation of the non-compliance referred to in paragraph 3 either immediately or within a reasonable time limit and shall take appropriate and proportionate measures with the aim of ensuring compliance.

(5) If a recognised data intermediation services provider or a recognised data altruism organisation does not comply with one or more of the requirements laid down in this Chapter even after having been notified in accordance with paragraph 3, that entity shall:

(a) lose its right to use the label referred to in Article 32a in written and spoken communication;

(b) be removed from the public Union register referred to in Article 32a.

Any decision revoking the right to use the label as referred to in the first subparagraph, point (a), shall be made public by the competent authority **and shall be notified to the Commission. The Commission shall remove the entity from the public Union register.**~~.~~

CHAPTER VIIb

Free flow of non-personal data **within**~~in~~ the Union'

Article 32h

Prohibition of localisation requirements for non-personal data within the Union

(1) Data localisation requirements for non-personal data shall be prohibited, unless they are justified on grounds of public security in compliance with the principle of proportionality or laid down on the basis of Union law.

(2) Member States shall immediately communicate to the Commission any draft act which introduces a new data localisation requirement or makes changes to an existing data localisation requirement in accordance with the procedures set out in Articles 5, 6 and 7 of Directive (EU) 2015/1535 of the European Parliament and of the Council.'

Chapter VIIc

Re-use of data and documents held by public sector bodies

Section 1

General Provisions

Article 32i

Subject matter and scope

(1) This Chapter establishes a set of rules governing the re-use and the practical arrangements for facilitating the re-use of the following:

(a) existing data and documents held by public sector bodies of the Member States, including certain categories of protected data;

(b) existing data and documents held by public undertakings that are:

(i) active in the areas referred to in Chapter II of Directive 2014/25/EU of the European Parliament and of the Council;

(ii) acting as public service operators pursuant to Article 2 of Regulation (EC) No 1370/2007 of the European Parliament and of the Council;

(iii) acting as air carriers fulfilling public service obligations pursuant to Article 16 of Regulation (EC) No 1008/2008 of the European Parliament and of the Council; or

(iv) acting as Community shipowners fulfilling public service obligations pursuant to Article 4 of Council Regulation (EEC) No 3577/92 ;

(c) research data pursuant to the conditions set out in Article 32t.

(2) This Chapter does not apply to the following:

(a) data and documents the supply of which is an activity falling outside the scope of the public task of the public sector bodies concerned as defined by law or by other binding rules in the Member State, or, in the absence of such rules, as defined in accordance with common administrative practice in the Member State in question, provided that the scope of the public tasks is transparent and subject to review;

(b) data and documents held by public undertakings and:

(i) produced outside the scope of the provision of services in the general interest as defined by law or other binding rules in the Member State;

(ii) related to activities directly exposed to competition and therefore, pursuant to Article 34 of Directive 2014/25/EU, not subject to procurement rules;

PUBLIC

(c) data and documents, such as sensitive data **or documents**, which are excluded from access by virtue of the access regimes in the Member State on grounds of the protection of national security (namely, State security), defence, or public security;

(d) data and documents held by public service broadcasters and their subsidiaries, and by other bodies or their subsidiaries for the fulfilment of a public service broadcasting remit.

(3) Section 2 of this Chapter does not apply to:

(a) data or documents, such as sensitive data or documents, which are excluded from access by virtue of the access regimes in the Member State, including on grounds of:

(i) statistical confidentiality;

(ii) commercial confidentiality (including business, professional or company secrets);

(b) data or documents access to which is restricted by virtue of the access regimes in the Member States,

(i) including cases whereby citizens or legal entities have to prove a particular interest to obtain access to documents;

(ii) on grounds of protection of personal data, **as well as**~~and~~ parts of data or documents accessible **under**~~by virtue of~~ those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the **legal framework for**~~law concerning~~ the protection of individuals with regard to the processing of personal data or as undermining the protection of privacy and the integrity of the individual, in particular **under**~~in accordance with~~ Union or national law regarding the protection of personal data; ~~logos, crests and insignia;~~

(c) logos, crests and insignia;

(d)~~(c)~~data or documents for which third parties hold intellectual property rights;

(e)~~(d)~~ data or documents held by cultural establishments other than libraries, including university libraries, museums and archives;

(f)~~(e)~~ data or documents held by educational establishments of secondary level and below, and, in the case of all other educational establishments, data other than those referred to in paragraph 1, point (c);

(g)~~(f)~~ data or documents other than those referred to in paragraph 1, point (c), held by research performing organisations and research funding organisations, including organisations established for the transfer of research results;

(h)~~(g)~~ **data**~~Data~~ or documents access to which is excluded or restricted on grounds of critical entity or critical infrastructure protection related information as defined in points (1) and (4) of Article 2 of Directive (EU) 2022/2557.

(4) Section 3 of this Chapter does not apply to:

(a) data ~~and documents~~ that are not certain categories of protected data;

(b) data or documents held by public undertakings;

(c) data or documents held by cultural establishments and educational establishments;

(d) data and documents covered by Section 2 of this Chapter.

~~(da)~~ **Section 3 does not create any obligation on public sector bodies to allow the re-use of data, nor does it release public sector bodies from their confidentiality obligations under Union or national law.**

(5) This Chapter builds on, and is without prejudice to, Union and national access regimes, in particular with regard to the granting of access to and disclosure of official **data or** documents.

(6) The obligations imposed in accordance with this Chapter shall apply only insofar as they are compatible with the provisions of international agreements on the protection of intellectual property rights, in particular the Berne Convention for the Protection of Literary and Artistic Works (Berne Convention), the Agreement on Trade-related

Aspects of Intellectual Property Rights (TRIPS Agreement and the World Intellectual Property Organization Copyright Treaty (WCT).

(7) The right for the maker of a database provided for in Article 7(1) of Directive 96/9/EC shall not be exercised by public sector bodies in order to prevent the re-use of data and documents or to restrict re-use beyond the limits set by this Chapter.

(8) This Chapter governs the re-use of existing data and documents held by public sector bodies and public undertakings of the Member States, including data and documents to which Directive 2007/2/EC of the European Parliament and of the Council applies.

(9) This Chapter is without prejudice to Union and national law and international agreements to which the Union or Member States are party on the protection of categories of data ~~or documents~~ referred to in Article 2(**53**~~54~~).

(10) This Chapter shall enter into application as of [24 months after the publication in the Official Journal of the European Union of this Regulation].

Article 32j

Non-discrimination

(1) Any applicable conditions for the re-use of data or documents shall be non-discriminatory, transparent, proportionate and objectively justified with regard to the categories of data or documents and the purposes of re-use and the nature of the data or documents for which re-use is allowed. Those conditions shall not be used to restrict competition. This principle shall equally apply for comparable categories of re-use, including for cross-border re-use.

(2) If data or documents are re-used by a public sector body as input for its commercial activities which fall outside the scope of its public tasks, the same charges and other conditions shall apply to the supply of the data or documents for those activities as the ones that apply to other re-users.

Article 32k

Exclusive arrangements

(1) The re-use of data or documents shall be open to all potential actors in the market, even if one or more market actors already exploit added-value products based on those data or documents. Agreements or other arrangements or practices pertaining to the re-use of data or documents, which have as their objective or effect to grant exclusive rights or to restrict the availability of data or documents for re-use by entities other than the parties to such agreements, arrangements or practices, shall be prohibited.

(2) By way of derogation of paragraph 1, where an exclusive right is necessary for the provision of a service of general interest, such a right may be granted to the extent necessary for the provision of the service or the supply of the product under the following conditions:

(a) the exclusive right is granted through an administrative act or contractual agreement in accordance with applicable Union and national law and in compliance with the principles of transparency, equal treatment and non-discrimination.

(b) the agreements **or administrative acts** granting the exclusive right, including the reasons as to why it is necessary to grant such a right, **shall be**~~is~~ transparent and **shall be** made publicly available online, in a form that complies with relevant Union law on public procurement and national law.

(c) except for exclusive rights related to the digitisation of cultural resources, the validity of the reason for granting exclusive rights concerning data and documents ~~**within the scope of Section 2**~~ shall be subject to regular review, and **for data and documents in scope of Section 2** shall in any event, be reviewed every three years.

(d) exclusive arrangements **concerning data and documents in Scope of Section 2** established on or after 16 July 2019 shall be made publicly available online at least two months before they come into effect. The final terms of such arrangements shall be transparent and shall be made publicly available online.

(3) By way of derogation of paragraph 1, where an exclusive right relates to the digitisation of cultural resources, the period of exclusivity shall in general not exceed

PUBLIC

10 years. Where that period exceeds 10 years, its duration shall be in accordance with applicable Union and national law subject to review during the 11th year and, if applicable, every seven years thereafter.

(4) In the case of an exclusive right referred to in paragraph 3, the public sector body concerned shall be provided free of charge with a copy of the digitised cultural resources as part of those arrangements. That copy shall be available for re-use at the end of the period of exclusivity.

(5) For certain categories of protected data, the duration of an exclusive right to re-use data shall not exceed 12 months. Where a contract is concluded **or administrative act is adopted**, the duration of the **arrangement**~~contract~~ shall be the same as the duration of the exclusive right.

(6) Agreements or other arrangements or practices that, without expressly granting an exclusive right, aim at, or could reasonably be expected to lead to, a restricted availability for the re-use of data and documents within the scope of Section 2 by entities other than parties to such **arrangements shall**~~arrangementsshall~~ be made publicly available online at least two months before their coming into effect. The effect of such legal or practical arrangements on the availability of data for re-use shall be subject to regular reviews and shall, in any event, be reviewed every three years. The final terms of such arrangements shall be transparent and made publicly available online.

(7) For existing exclusive arrangements, the following shall apply:

(a) exclusive arrangements concerning data and documents within the scope of Section **2 existing**~~2existing~~ on 17 July 2013 that do not qualify for the exceptions set out in paragraphs 2 and 3 and that were entered into by public sector bodies shall be terminated at the end of the contract and in any event not later than 18 July 2043;

(b) exclusive arrangements concerning data and documents within the scope of Section 2 existing on 16 July 2019 that do not qualify for the exceptions set out in paragraphs 2 and 3, and that were entered into by public undertakings, shall

be terminated at the end of the contract and in any event not later than 17 July 2049;

Article 32l

General principles relating to charging

(1) Any charges set out under Section 2 or Section 3 shall be transparent, non-discriminatory, proportionate and objectively justified and shall not restrict competition.

(2) In the case of standard charges for the re-use of data or documents, any applicable conditions and the actual amount of those charges, including the calculation basis for such charges, shall be established in advance and published, through electronic means ~~**where possible and appropriate**~~.

(3) In the case of charges for the re-use other than those referred to in paragraph **2**~~**1**~~, the factors that are taken into account in the calculation of those charges shall be indicated at the outset. Upon request, the holder of the data or documents in question shall also indicate the way in which such charges have been calculated in relation to a specific re-use request.

(4) Public sector bodies shall ensure that any charges can also be paid online through widely available cross-border payment services, without discrimination based on the place of establishment of the payment service provider, the place of issue of the payment instrument or the location of the payment account within the Union.

~~4a.~~ **Article 32la**

~~4b.~~ **Procedure for re-quests for re-use**

~~4c.~~ **(1) Public sector bodies shall, through electronic means where possible and appropriate, process requests for re-use and shall make the data or document available for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant within a reasonable time that is consistent with the time frames laid down for the processing of requests for access to data or documents.**

PUBLIC

(2) **(a) Public sector bodies shall process the request for re-use of data and documents in scope of Section II of this Chapter and, in case of a positive decision, shall deliver the data or documents to the applicant or, if a licence is needed, finalise the licence offer to the applicant as soon as possible and in principle within 20 working days of receipt. That time frame may be extended by a further 20 working days in the case of extensive or complex requests.**

~~4e.~~ **(b) Public sector bodies or the competent bodies referred to in paragraph 1 of Article 32z shall adopt a decision on the request for re-use of certain categories of protected data as soon as possible and in any event within two months of receipt and, in the case of a positive decision, shall grant access to the protected data for re-use in accordance with the modalities referred to in Article 32w, where possible. In the case of exceptionally extensive and complex requests for re-use, the two-month period to adopt a decision may be extended by up to 30 days.** ~~The time limit for granting access may be extended within reasonable limits.~~

(2a) **Where time limits under paragraph 2 are extended, the public sector body and in the case of certain categories of protected data the competent body shall notify the applicant as soon as possible, and in any event within three weeks of the initial request, stating the reasons.**

(3) **In the event of a negative decision, the public sector bodies or competent bodies where relevant, shall communicate the grounds for refusal to the applicant on the basis of the relevant provisions of the access regime in that Member State or the provisions of this Regulation. Where a negative decision is based on point (d) of paragraph 3 of Article 32i, the public sector body or competent body shall include a reference to the natural or legal person who is the rightsholder, where known, or alternatively to the licensor from which the public sector body has obtained the relevant material. Libraries, including university libraries, museums and archives, shall not be required to include such a reference.**

~~4h.~~ **(4) Any natural or legal person directly affected by a decision as referred to in paragraph 12 or 3 shall have an effective right of redress in the Member State where the relevant body is located. Such a right of redress shall be laid down in national law and shall include the possibility of review by an impartial body**

with the appropriate expertise, such as the national competition authority, the relevant access-to-documents authority, the supervisory authority established in accordance with Regulation (EU) 2016/679 or a national judicial authority, whose decisions are binding upon the public sector body or the competent body concerned.

~~4i.~~ **(5) Where the request for re-use relates to data and documents in scope of Section 2 of this Chapter, this article shall not apply to the following entities:**

~~4h.~~ **(a) public undertakings;**

~~4i.~~ **(b) educational establishments, research performing organisations and research funding organisations.**

Article 32m

Information on means of redress

Public sector bodies shall ensure that applicants for re-use of data or documents are informed of available means of redress relating to decisions or practices affecting them. **Any decision on re-use shall contain a reference to the means of redress by which the applicant may challenge the decision.**

Section 2

Re-use of **public sector** open ~~government~~ data

Subsection 1

Scope and General Principles

Article 32n

General principle for re-use of **public sector** open ~~government~~ data

(1) Data or documents in scope of this Section shall be re-usable for commercial or non-commercial purposes in accordance with Section 1 and Section 2 Subsection **2**~~3~~.

(2) For data or documents in which libraries, including university libraries, museums and archives hold intellectual property rights and for data or documents held by public

undertakings, where the re-use of such data or documents is allowed, those data or documents shall be re-usable for commercial or non-commercial purposes in accordance with Section 1 and Section 2 Subsection 23.

~~**Subsection 2**~~

~~**Requests for re-use**~~

~~**Article 32o**~~

~~**Processing requests for re-use**~~

~~(1)~~ ~~**Public sector bodies shall, through electronic means where possible and appropriate, process requests for re-use and shall make the document available for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant within a reasonable time that is consistent with the time frames laid down for the processing of requests for access to data or documents.**~~

~~(2)~~ ~~**Where no time limits or other rules regulating the timely provision of data or documents have been established, public sector bodies shall process the request and shall deliver the data or documents for re-use to the applicant or, if a licence is needed, finalise the licence offer to the applicant as soon as possible, and in any event within 20 working days of receipt. That time frame may be extended by a further 20 working days in the case of extensive or complex requests. In such cases, the applicant shall be notified as soon as possible, and in any event within three weeks of the initial request, that more time is needed to process the request and the reasons why.**~~

~~(3)~~ ~~**In the event of a negative decision, the public sector bodies shall communicate the grounds for refusal to the applicant on the basis of the relevant provisions of the access regime in that Member State or the provisions of this Regulation, in particular points (a) to (c) of paragraph 2 of Article 32i and points (a) to (d) of paragraph 3 of Article 32i or Article 32n (general principle ODD Section). Where a negative decision is based on point (d) of paragraph 3 of Article 32i, the public sector body shall include a reference to the natural or legal person who is the rightsholder, where known, or alternatively to the licensor from which the public sector body has obtained the relevant material. Libraries,**~~

PUBLIC

~~including university libraries, museums and archives, shall not be required to include such a reference.~~

~~(4) The means of redress shall include the possibility of review by an impartial review body with the appropriate expertise, such as the national competition authority, the relevant access to data or documents authority, the supervisory authority established in accordance with Regulation (EU) 2016/679 or a national judicial authority, whose decisions are binding upon the public sector body concerned.~~

~~(5) For the purposes of this Article, Member States shall establish practical arrangements to facilitate effective re-use of data or documents. Those arrangements may in particular include the means to supply adequate information on the rights provided for in this Regulation and to offer relevant assistance and guidance.~~

~~(6) This Article shall not apply to the following entities:~~

~~(a) public undertakings;~~

~~(b) educational establishments, research performing organisations and research funding organisations.~~

Subsection **2**~~3~~

Conditions for re-use

Article 32p

Available formats

(1) Without prejudice to Subsection 5, public sector bodies and public undertakings shall make their data ~~or documents~~ available in any pre-existing format or language ~~and, where possible and appropriate,~~ by electronic means, in formats that are open, machine-readable, accessible, findable and re-usable, together with their metadata. Both the format and the metadata shall, where possible, comply with formal open standards. **Public sector bodies and public undertakings shall make their documents available in any pre-existing format or language.**

(2) **Wherever possible and appropriate,** ~~**Member States shall encourage**~~ public sector bodies and public undertakings **shall** ~~**to**~~ produce and make available data or documents falling within the scope of this Section in accordance with the principle of 'open by design and by default**'**.

(3) Paragraph 1 shall not imply an obligation for public sector bodies to create or adapt data or documents or provide extracts in order to comply with that paragraph where this would involve disproportionate effort, going beyond a simple operation.

(4) Public sector bodies shall not be required to continue the production and storage of a certain type of **data or** document with a view to the re-use of such data or documents by a private or public sector organisation.

(5) Public sector bodies shall make dynamic data available for re-use immediately after collection, via suitable APIs and, where relevant, as a bulk download.

(6) Where making dynamic data available for re-use immediately after collection, as referred to in paragraph 5, would exceed the financial and technical capacities of the public sector body, thereby imposing a disproportionate effort, those dynamic data shall be made available for re-use within a time frame or with temporary technical restrictions that do not unduly impair the exploitation of their economic and social potential.

(7) Paragraphs 1 to 6 shall apply to existing data or documents held by public undertakings which are available for re-use.

(8) The high-value datasets, as listed in accordance with Article 32v(1) shall be made available for re-use in machine- readable format, via suitable APIs and, where relevant, as a bulk download.'

Article 32q

Principles governing charging for **public sector** open ~~**government**~~ data

(1) The re-use of data or documents within the scope of this Section shall be free of charge. However, the recovery by the public sector body holding the data **or documents** of the marginal costs incurred for the reproduction, provision**, extensive**

searches and dissemination of such data or documents as well as for anonymisation of personal data and measures taken to protect commercially confidential information **and other information protected by law** may be allowed.

(2) Paragraph 1 shall not apply to the following entities:

(a) public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks;

(b) libraries, including university libraries, museums and archives;

(c) public undertakings.

(3) Member States shall publish online a list of the public sector bodies referred to in paragraph 2, point (a).

(4) In the cases referred to in paragraph 2, points (a) and (c), the total charges shall be calculated in accordance with objective, transparent and verifiable criteria. Such criteria shall be laid down by Member States. The total income from supplying and allowing the re-use of data or documents over the appropriate accounting period shall not exceed the cost of their collection, production, reproduction, dissemination and data storage, together with a reasonable return on investment, and where applicable, the anonymisation of personal data and measures taken to protect commercially confidential information. Charges shall be calculated in accordance with the applicable accounting principles.

(5) Where charges are made by the public sector bodies referred to in paragraph 2, point (b), the total income from supplying and allowing the re-use of data or documents over the appropriate accounting period shall not exceed the cost of collection, production, reproduction, dissemination, data storage, preservation and rights clearance and, where applicable, the anonymisation of personal data and measures taken to protect commercially confidential information, together with a reasonable return on investment. Charges shall be calculated in accordance with the accounting principles applicable to the public sector bodies involved.

(6) **Charges**~~Public sector bodies may set out~~ higher **than the** charges **provided for in paragraphs 1, 4 and 5 may be set out** for the re-use of data and documents by very

PUBLIC

large enterprises ~~than the charges provided for in paragraphs 1, 4 and 5~~. Any such charges shall be proportionate and based on objective criteria, taking into account the economic power, or the ability of the entity to acquire data **or documents**, including in particular a designation as a gatekeeper under Regulation (EU) 2022/1925. In addition to the elements listed in paragraph 1 of this Article, such charges may cover the cost of collection, production, reproduction dissemination and data storage and where applicable the cost of anonymisation or measures to protect the confidentiality of the data or documents, together with a reasonable return on investment.

(7) The re-use of the following shall be free of charge for the **re-user**~~user~~:

(a) subject to Article 32v paragraph (3), (4) and (5), the high-value datasets, as listed in accordance with paragraph 1 of that Article;

(b) research data referred to in point (c) of paragraph 1 of Article 32i.

Article 32r

Standard licences

(1) The re-use of data or documents shall not be subject to conditions, unless such conditions are objective, proportionate, non-discriminatory and justified on grounds of a public interest objective.

(2) When re-use is subject to conditions, those conditions shall not unnecessarily restrict possibilities for re-use and shall not be used to restrict competition.

(3) In Member States where licences are used, public sector bodies **and public undertakings** shall ensure that the standard licences for the re-use of public sector data or documents, which can be adapted to meet particular licence applications, are available in digital format and able to be processed electronically.

(4) Public sector bodies **and public undertakings** may establish special conditions for the re-use of data and documents by very large enterprises. Such conditions shall be proportionate and should be based on objective criteria. They shall be established taking into consideration the economic power, or the ability of the entity to acquire

data **and documents**, including in particular a designation as a gatekeeper under Regulation (EU) 2022/1925.

Article 32s

Practical arrangements

(1) Member States shall make practical arrangements facilitating the search for data or documents available for re-use, such as asset lists of main data or documents with relevant metadata, accessible where possible and appropriate online and in machine-readable format, and **on data portals**~~portal sites~~ that are linked to the asset lists. Where possible, Member States shall facilitate the cross-linguistic search for data or documents, in particular by enabling metadata aggregation at Union level.

Member States shall also encourage public sector bodies to make practical arrangements facilitating the preservation of data **and**~~or~~ documents available for re-use.

(2) Member States shall, in cooperation with the Commission, **ensure simple**~~continue efforts to simplify~~ access to datasets, in particular by providing a single point of access and by progressively making available suitable datasets held by public sector bodies with regard to the data or documents to which this Section applies, as well as to data **and documents** held by Union institutions, in formats that are accessible, readily findable and re-usable by electronic means.

Subsection **3**~~4~~

Research data

Article 32t

Research data

(1) Member States shall support the availability of research data by adopting national policies and relevant actions aiming at making publicly funded research data openly available (‘open access policies’), following the principle of ‘open by default’ and compatible with the FAIR principles. In that context, concerns relating to intellectual property rights, personal data protection and confidentiality, security and legitimate commercial interests, shall be taken into account in accordance with the principle of

'as open as possible, as closed as necessary'. Those open access policies shall be addressed to research performing organisations and research funding organisations.

(2) Without prejudice to Article **32i**~~32n~~, paragraph 3, point (d), research data shall be re-usable for commercial or non-commercial purposes in accordance with Section 1 and Section 2 Subsection **2**~~3~~, insofar as they are publicly funded and researchers, research performing organisations or research funding organisations have already made them publicly available through an institutional or subject-based repository. In that context, legitimate commercial interests, knowledge transfer activities and pre-existing intellectual property rights shall be taken into account.

Subsection **4**~~5~~

High-value datasets

Article 32u

Thematic categories of high-value datasets

(1) The thematic categories of high-value datasets shall be as set out in Annex I.

(2) The Commission is empowered to adopt delegated acts in accordance with Article **45(2)**~~45(2a)~~ in order to amend Annex I by adding new thematic categories of high-value datasets reflecting technological and market developments.

Article 32v

Specific high-value datasets and arrangements for publication and re-use

(1) The Commission shall adopt implementing acts laying down a list of specific high-value datasets belonging to the categories set out in Annex I and held by public sector bodies and public undertakings among the data or documents to which this Section applies.

Such specific high-value datasets shall be:

(a) available free of charge, subject to paragraphs 3, ~~4 and 5~~**and 4**;

(b) machine readable;

(c) provided via APIs; and

(d) provided as a bulk download, where relevant.

Those implementing acts may specify the arrangements for the publication and re-use of high-value datasets. Such arrangements shall be compatible with open standard licences.

The arrangements may include terms applicable to re-use, formats of data and metadata and technical arrangements for dissemination. Investments made by the Member States in open data approaches, such as investments into the development and roll-out of certain standards, shall be taken into account and balanced against the potential benefits from inclusion in the list.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).

(2) The identification of specific high-value datasets pursuant to paragraph 1 shall be based on the assessment of their potential to:

(a) generate significant socioeconomic or environmental benefits and innovative services;

(b) benefit a high number of users, in particular SMEs and SMCs;

(c) assist in generating revenues; and

(d) be combined with other datasets.

For the purpose of identifying such specific high-value datasets, the Commission shall carry out appropriate consultations, including at expert level, conduct an impact assessment and ensure complementarity with existing legal acts, such as **Directive 2007/2/EC and** Directive 2010/40/EU of the European Parliament and of the Council, with respect to the re-use of data or documents. That impact assessment shall include a cost-benefit analysis and an analysis of whether providing high-value datasets free of charge by public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks would lead to a substantial impact on the budget of such bodies. With regard to high-value datasets

PUBLIC

held by public undertakings, the impact assessment shall give special consideration to the role of public undertakings in a competitive economic environment.

(3) By way of derogation from paragraph 1, second subparagraph, point (a), the implementing acts referred to in that paragraph shall provide that the availability of high-value datasets free of charge is not to apply to specific high-value datasets held by public undertakings where that would lead to a distortion of competition in the relevant markets.

(4) The requirement to make high-value datasets available free of charge pursuant to point (a) of the second subparagraph of paragraph 1 shall not apply to libraries, including university libraries, museums and archives.

~~(5) Where making high-value datasets available free of charge by public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks would lead to a substantial impact on the budget of the bodies involved, Member States may exempt those bodies from the requirement to make those high-value datasets available free of charge for a period of no more than two years following the entry into force of the relevant implementing act adopted in accordance with paragraph 1.~~

Section 3

Re-use of certain categories of protected data held by public sector bodies

Article 32w

Conditions for re-use **of certain categories of protected data**

(1) Public sector bodies which are competent under national law to grant or refuse access for the re-use of ~~data or documents belonging to~~ certain categories of protected data shall make publicly available the conditions for allowing such re-use and the procedure to request the re-use via the single information point referred to in Article 32aa. Where they grant or refuse access for re-use, they may be assisted by the competent bodies referred to in Article 32z (1).

Member States shall ensure that public sector bodies are equipped with the necessary resources to comply with this Article and Article 32x.

(2) Re-use of **certain categories of protected** data ~~or documents~~ shall not affect the protected nature of those data or documents and shall only be allowed:

(a) in compliance with intellectual property rights.

(b) if data ~~or documents~~ **that are** ~~that is~~ considered confidential in accordance with Union or national law on commercial or statistical confidentiality, **are** ~~is~~ not disclosed, as a result of allowing re-use, unless such re-use is allowed based on the data ~~subject's consent or the data~~ holder's permission in accordance with paragraph 5.

(c) in compliance with Regulation (EU) 2016/679.

(3) To ensure the preservation of the protected nature as referred to in paragraph 2, public sector bodies may establish the following requirements:

(a) to grant access for the re-use of data ~~or documents~~ only where the public sector body or the competent body, following the request for re-use, has ensured that those data ~~or documents~~ have been:

(i) anonymised, in the case of personal data;

~~(ii) subject to other forms of preparation of personal data;~~

(iii) modified, aggregated or treated by any other method of disclosure control, in the case of commercially confidential information, including trade secrets or content protected by intellectual property rights;

(b) to access and re-use the data ~~or documents~~ remotely within a secure processing environment that is provided or controlled by the public sector body;

(c) to access and re-use the data ~~or documents~~ within the physical premises in which the secure processing environment is located in accordance with high

PUBLIC

security standards, provided that remote access cannot be allowed without jeopardising the rights and interests of third parties.

In the case of re-use allowed in accordance with the first subparagraph, point (a)(i), the re-use of data or documents shall be subject to the rules on **public sector** open ~~government~~ data set out in Section 2. This is without prejudice to Article 32y, which prevails in case of conflict.

In the case of re-use allowed in accordance with the first subparagraph, points (b) and (c), the public sector bodies shall impose conditions that preserve the integrity of the functioning of the technical systems of the secure processing environment used.

(4) The public sector body shall reserve the right to verify the process, the means and any results of processing of **certain categories of** data ~~or documents~~ undertaken by the re-user to preserve the integrity of the protection of the data ~~or documents~~. It shall also reserve the right to prohibit the use of results that contain information jeopardising the rights and interests of third parties. The decision to prohibit the use of the results shall be comprehensible and transparent to the re-user.

(4a) Unless national law provides for specific safeguards on applicable confidentiality obligations relating to the re-use of certain categories of protected data, the public sector body shall make the re-use of data ~~or documents~~ provided in accordance with paragraph 3 conditional on the adherence by the re-user to a confidentiality obligation that prohibits the disclosure of any information that jeopardises the rights and interests of third parties and that the re-user may have acquired despite the safeguards put in place. **Re-users shall be prohibited from re-identifying any data subject and shall take technical and operational measures to prevent re-identification and to notify any data breach resulting in the re-identification of the data subjects concerned to the public sector body.** In the event of the unauthorised re-use of non-personal data, the re-user shall be obliged, without delay, where appropriate with the assistance of the public sector body, to inform the natural or legal persons whose rights and interests may be affected.

(5) Where the re-use of data **that are protected on the grounds of commercial or statistical confidentiality or of intellectual property rights of third parties** ~~or~~

~~documents~~ cannot be allowed in accordance with paragraphs 3 and 4, re-use shall only be possible:

~~(a) where there is no legal basis other than consent for transmitting the data under Regulation (EU) 2016/679, with the consent of the data subjects;~~

~~(b)~~ with the permission from the data holders whose rights and interests may be affected by such re-use.

The public sector body shall make best efforts, in accordance with Union and national law, to provide assistance to potential re-users in seeking ~~consent of the data subjects or~~ permission from the data holders whose rights and interests may be affected by such re-use, where this is feasible without a disproportionate burden on the public sector body. –

Where it provides such assistance, the public sector body may be assisted by the competent bodies referred to in Article 32z.

Article 32x

Requirements for transfers of non-personal **protected** data to third countries by re-users

(1) Where a re-user intends to transfer certain categories of protected data that are non-personal to a third country, it shall inform the public sector body of its intention to transfer such data and the purpose of such transfer at the time of requesting the re-use ~~of the data~~. In the case of re-use based on the data holder's permission the re-user shall, where appropriate with the assistance of the public sector body, inform the natural or legal person whose rights and interests may be affected of that intention, purpose and the appropriate safeguards. The public sector body shall not allow the re-use unless the natural or legal person gives permission for the transfer.

(2) Public sector bodies shall transmit non-personal confidential data or data protected by intellectual property rights to a re-user which intends to transfer those data to a third country other than a country designated in accordance with paragraph **5**~~7~~ only if the re-user contractually commits to:

(a) complying with the obligations imposed in accordance with intellectual property rights and Union or national law on commercial or statistical confidentiality even after the data is transferred to the third country;

(b) accepting the jurisdiction of the courts or tribunals of the Member State of the transmitting public sector body with regard to any dispute related to compliance with intellectual property rights and Union or national law on commercial or statistical confidentiality.

(3) The Commission may adopt implementing acts establishing model contractual clauses for complying with the obligations referred to in paragraph 2 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).

(4) Public sector bodies shall, where relevant and to the extent of their capabilities, provide guidance and assistance to re-users in complying with the obligations referred to in paragraph 2.

(5) Where justified because of the substantial number of requests across the Union concerning the re-use of non- personal data in specific third countries, the Commission may adopt implementing acts declaring that the legal, supervisory and enforcement arrangements of a third country:

(a) ensure protection of intellectual property and trade secrets in a way that is essentially equivalent to the protection ensured under Union law;

(b) are being effectively applied and enforced; and

(c) provide effective judicial redress.

(6) Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).

(7) Specific Union legislative acts may deem certain non-personal data categories held by public sector bodies to be highly sensitive for the purposes of this Article where their transfer to third countries may put at risk Union public policy objectives, such as safety and public health or may lead to the risk of re-identification of non-personal, anonymised data. Where such an act is adopted, the Commission shall

PUBLIC

adopt delegated acts in accordance with Article 45 supplementing this Regulation by laying down special conditions applicable to the transfers of such data to third countries.

Those special conditions shall be based on the nature of the non-personal data categories identified in the specific Union legislative act and on the grounds for deeming those categories to be highly sensitive, taking into account the risks of re-identification of non-personal, anonymised data. They shall be non-discriminatory and limited to what is necessary to achieve the Union public policy objectives identified in that act, in accordance with the Union's international obligations.

If required by a specific Union legislative act referred to in the first subparagraph, such special conditions may include terms applicable for the transfer or technical arrangements in this regard, limitations with regard to the re-use of data in third countries or categories of persons entitled to transfer such data to third countries or, in exceptional cases, restrictions with regard to transfers to third countries.

The re-user to whom the right to re-use non-personal data was granted may transfer the data only to those third countries for which the requirements set out in paragraphs 2, **5 and 7**~~4 and 5~~ are met.

Article 32y

Fees **for the re-use of certain categories of protected data**

(1) Public sector bodies which allow re-use of certain categories of protected data may charge fees for allowing the re-use of such data.

(2) Where ~~public sector bodies charge~~ fees **are charged, Member States**~~, they~~ shall take measures to provide incentives for the re-use of certain categories of protected data for non-commercial purposes, such as scientific research purposes, and by start-ups, SMEs and SMCs in accordance with Union State aid rules. In that regard, public sector bodies may ~~also~~ make the data available at a discounted fee or free of charge, in particular to start-ups, SMEs and SMCs, civil society, research and educational establishments. To that end, ~~public sector bodies may establish~~ a list of categories of re-users to which data ~~or documents~~ for re-use is made available at a discounted

fee or free of charge **may be established**. That list, together with the criteria used to establish it, shall be made public.

(3) Any fees shall be derived from the costs related to conducting the procedure for requests for the re-use of certain categories of protected data and limited to the necessary costs in relation to:

(a) the reproduction, provision and dissemination of data;

(b) the clearance of rights;

(c) anonymisation ~~or other forms of preparation~~ of personal data and **preparation of** commercially confidential data as provided for in Article 32w(3)~~[conditions for re-use]~~;

(d) the maintenance of the secure processing environment;

(e) the acquisition of the right to allow re-use in accordance with this Section by third parties outside the public sector; and ~~assisting re-users in seeking consent from data subjects and permission from data holders whose rights and interests may be affected by such re-use.~~

(f) assisting re-users in seeking consent from data subjects and permission from data holders whose rights and interests may be affected by such re-use.

(4) The criteria and methodology for calculating fees shall be laid down by the Member States and published. The public sector body shall publish a description of the main categories of costs and the rules used for the allocation of costs.

(5) Public sector bodies may charge higher fees than those allowed in accordance with paragraph 2 and 3 of this Article with respect to very large enterprises, based on objective criteria, taking into account the economic power, or the ability of the entity to acquire data, including in particular a designation as a gatekeeper under Regulation (EU) 2022/1925. Any such calculated fees shall be proportionate. In addition to the elements listed in paragraph 3 of this Article, they can cover the cost of collection and production of the data, together with a reasonable return on investment.

Article 32z

Competent bodies

(1) For the purpose of carrying out the tasks referred to in this Article, each Member State shall designate one or more competent bodies ~~in accordance with Article 37(1)~~, which may be competent for particular sectors, but that collectively need to cover all sectors, to assist the public sector bodies which grant or refuse access for the re-use of certain categories of protected data. Member States may either establish one or more ~~new~~ competent bodies or rely on existing public sector bodies or on internal services of public sector bodies that fulfil the conditions laid down in this Section.

(2) The competent bodies may be empowered to grant access for the re-use of certain categories of protected data pursuant to Union or national law which provides for such access to be granted. ~~Where they grant or refuse access for re-use, those competent bodies shall be subject to Articles 32k, 32w, 32x, 32y and 32ab.~~

~~(3) The competent bodies shall have adequate legal, financial, technical and human resources to carry out the tasks assigned to them, including the necessary technical knowledge to be able to comply with relevant Union or national law concerning the access regimes for the categories of protected data referred to in in Article 2(54).~~

(3)~~(4)~~ The assistance referred to in paragraph 1 shall include, where necessary:

(a) providing technical support by making available a secure processing environment for providing access for the re-use of **certain categories of protected** data ~~or documents~~;

(b) providing guidance and technical support on how to best structure and store **certain categories of protected** data to make ~~that~~ those data ~~or documents~~ easily accessible;

(c) providing technical support for anonymization, pseudonymisation and state-of-the-art privacy-preserving methods~~. not limited to personal data, but also to~~**,**

and the commercially confidential information, including trade secrets or content protected by intellectual property rights;

(d) assisting the public sector bodies, where relevant, to provide support to re-users in requesting consent for re-use from data subjects or permission from data holders in line with their specific decisions, including on the jurisdiction in which the data processing is intended to take place and assisting the public sector bodies in establishing technical mechanisms that allow the transmission of requests for consent or permission from re-users, where practically feasible;

(e) providing public sector bodies with assistance in assessing the adequacy of contractual commitments made by a re-user pursuant to Article 32x(2).

Article 32aa

Single information point

(1) Each Member State shall designate a single information point. That point shall make available easily accessible information concerning the application of Articles 32w, 32x and 32y. **The single information point may be linked to sectoral, regional or local information points.**

(2) The single information point shall be competent to receive enquiries or requests for the re-use of the certain categories of protected data and shall transmit them, where possible and appropriate by automated means, to the competent public sector bodies, or the competent bodies referred to in Paragraph 1 of Article 32z, where relevant.

(3) The single information point may include a separate, simplified and well-documented information channel for SMEs, SMCs, start-ups and research establishments addressing their needs and capabilities in requesting the re-use of **certain** ~~the~~ categories of data referred to in Article 2(**53**~~54~~).

(4) The single information point shall make available by electronic means a searchable asset list containing an overview of all available **data**~~document~~ resources including, where relevant, those **data**~~document~~ resources that are available at sectoral, regional or local information points~~,~~ with relevant information describing the available data

~~or documents~~, including at least ~~the data format and size and~~ the conditions for their re-use.

(5) The Commission shall establish a European single access point offering a searchable electronic register of data ~~or documents~~ available in the national single information points and further information on how to request data ~~or documents~~ via those national single information points.

~~Article 32ab~~

~~Procedure for requests for re-use~~

~~(1) Unless shorter time limits have been established in accordance with national law, the competent public sector bodies or the competent bodies referred to in paragraph 1 of Article 32z shall adopt a decision on the request for the re-use of certain categories of protected data within two months of the date of receipt of the request.~~

~~(2) In the case of exceptionally extensive and complex requests for re-use, that two-month period may be extended by up to 30 days. In such cases the competent public sector bodies or the competent bodies referred to in paragraph 1 of Article 32z shall notify the applicant as soon as possible that more time is needed for conducting the procedure, together with the reasons for the delay.~~

~~(3) Any natural or legal person directly affected by a decision as referred to in paragraph 1 shall have an effective right of redress in the Member State where the relevant body is located. Such a right of redress shall be laid down in national law and shall include the possibility of review by an impartial body with the appropriate expertise, such as the national competition authority, the relevant access-to-documents authority, the supervisory authority established in accordance with Regulation (EU) 2016/679 or a national judicial authority, whose decisions are binding upon the public sector body or the competent body concerned.~~

18aa. Article 33 is amended as follows:

(a) Point (d) in paragraph 1 is replaced by the following:

~~3c.~~ **'where applicable, the means to enable the interoperability of tools for automating the execution of data sharing agreements shall be provided.'**

(b) the second subparagraph of paragraph 2 is replaced as follows:

~~3e.~~ **'The Commission shall when adopting delegated acts take into account the advice of the EDIB.**

18a. Article 37 is amended as follows:

~~3g.~~ **(a) Paragraph (1) is replaced by the following:**

(1) 'Each Member State shall designate one or more competent authorities to be responsible for the application and enforcement of this Regulation, with exception of Chapters VIIb and VIIc (competent authorities). Member States may establish one or more new authorities or rely on existing authorities.'

~~3i.~~ **(b) paragraph 3 is replaced by the following:**

~~3j.~~ **The supervisory authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall be responsible for monitoring the application of this Regulation insofar as the protection of personal data is concerned.**
The European Data Protection Supervisor shall be responsible for monitoring the application of this Regulation insofar as it concerns the Commission, the European Central Bank or Union bodies.
The tasks and powers of the supervisory authorities referred to in this paragraph shall be exercised with regard to the processing of personal data.

~~3e.~~

~~3f.~~

~~3g.~~

~~3m.~~ **(c) paragraph 5 is amended as follows:**

~~3n.~~ **(-i) point f is replaced by the following:**

PUBLIC

~~3o.~~ **'(f) cooperating with competent authorities of other Member States and, where relevant, with the Commission, or the EDIB, or BEREC, to ensure the consistent and efficient application of this Regulation, including the exchange of all relevant information by electronic means, without undue delay, including regarding paragraph 10 of this Article;'**

~~3p.~~ **(ii) point g is replaced by the following:**

~~3q.~~ **'(g) cooperating with the relevant competent authorities responsible for the implementation of other Union or national legal acts, including with authorities competent in the field of data and electronic communication services, with the supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679 or with sectoral authorities to ensure that this Regulation is enforced consistently with other Union and national law, including the exchange of all relevant information;'**

(d) paragraph 17 is added:

17. 'BEREC shall facilitate regular exchanges among national competent authorities responsible for the application and enforcement of Articles 23 to 31 and Articles 34 and 35 of this Regulation and shall collect and disseminate, among those national competent authorities, best practices for the application and enforcement of those articles.'

19. Article 38 is replaced by the following:

'(1) Without prejudice to any other administrative or judicial remedy, natural and legal persons shall have the right to lodge a complaint, individually or, where relevant, collectively:

(a) with the relevant competent authority in the Member State of their habitual residence, place of work or establishment if they consider that their rights under this Regulation have been infringed;

(b) any matter falling within the scope of this Regulation specifically against a recognised data intermediation services provider or a recognised data altruism organisation, with the relevant competent authority for the registration of data

intermediation services or the relevant competent authority for the registration of data altruism organisations.

(2) The data coordinator shall, upon request, provide all the necessary information to natural and legal persons for the lodging of their complaints with the appropriate competent authority.

(3) The competent authority with which the complaint has been lodged shall inform the complainant, in accordance with national law, of:

(a) the progress of the proceedings, of the decision taken; and

(b) the judicial remedies provided for in Article 39.

(4) Competent authorities shall cooperate to handle and resolve complaints effectively and in a timely manner, including by exchanging all relevant information by electronic means, without undue delay. This cooperation shall not affect the cooperation mechanisms provided for by Chapters VI and VII of Regulation (EU) 2016/679 and by Regulation (EU) 2017/2394.

(5) This Article shall not apply to Chapters VIIb and VIIc.'

19a. in Article 39, paragraph (4) is inserted:

'(4) This Article shall not apply to Chapters VIIb and VIIc.''

20. ~~in~~ Article 40, paragraph **(4) is replaced by the following**~~(6) is inserted~~:

'(4)~~6.~~ This Article shall not apply to Chapter **VIIb and** VIIc.

(b) paragraph 5 is deleted. '

21. after Article 41, the following heading is inserted:

'CHAPTER IXa

European Data Innovation Board;'

22. the following Article 41a is inserted:

‘Article 41a

European Data Innovation Board

(1) The European Data Innovation Board is established as a means to advising and assisting the Commission in coordinating the enforcement of this Regulation and to serve as a forum of **strategic** discussion for the development of a European data economy and data policies.

(2) It shall be composed at least of representatives of Member States competent for matters related to data, the competent authorities for enforcement of Chapters II, III, V, VIIa **of this Regulation and representatives' of Member States' authorities overseeing or competent bodies supporting the implementation of Chapter** ~~and~~ VIIc of this Regulation, the European Data Protection Board, the European Data Protection Supervisor, ENISA, the EU SME Envoy or a representative appointed by the network of SME envoys**. If a Member State has designated more than one competent authority or competent body, they are represented in the plenary meetings of the Board by the designated data coordinator. Other competent authorities or competent bodies entrusted with specific operational responsibilities for the application and enforcement of this Regulation may participate in the thematic subgroups of the Board relevant for their responsibilities**. The Commission may decide to add additional categories of members. In its appointments of individual experts, the Commission shall aim to achieve gender and geographical balance among the members of the group.

(3) The Commission shall decide on the composition of the different configurations in which the Board will fulfil its tasks.

(4) The Commission shall chair the meetings of the European Data Innovation Board.’

23. Article 42 is replaced by the following:

‘Article 42

Role of the EDIB

(1) The EDIB shall support the consistent application of this Regulation by:

(a) serving as a forum for strategic discussions on data policies, data governance, international data flows and cross-sectoral developments relevant to the European data economy;

(b) advising and assisting the Commission with regard to developing consistent practice of competent authorities in the enforcement of Chapters II, III, V, VII, VIIa and VIIc;

(c) facilitating cooperation between competent authorities through capacity-building and the exchange of information;

(d) fostering an exchange of experience and good practice between the Member States in the field of re-use of public sector information in collaboration with other relevant governance bodies.;

(e) advising and assisting the Commission with regard to the implementation of Chapters II, III, V, VII, VIIa and VIIc by suggesting development of guidance for businesses and public organisations;

(f) advising and assisting the Commission on cross-sector standardisation issues;

(g) ensuring active cooperation and coordination with other relevant bodies, and expert groups to ensure policy consistency in the digital single market.';'

24. Article 45 is amended as follows:

(a) paragraph 2 is replaced by the following:

'2. The power to adopt delegated acts referred to in Article 29(7), Article 32u(2)**, Article 32x(7),** and Article 33(2) shall be conferred on the Commission for an indeterminate period of time.'

(b) paragraph 3 is replaced by the following:

'3. The delegation of power referred to in Article 29(7), Article 32u(2)**, Article 32x(7),** and Article 33(2) may be revoked at any time by the European

Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.'

(c) paragraph 6 is replaced by the following:

'6. A delegated act adopted pursuant to Article 29(7), Article 32u(2), **Article 32x(7),** or Article 33(2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of three months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.'

25. Article 46 is amended as follows:

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

'The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.'

(b) the following paragraph 1a is inserted:

'1a. Where reference is made to this paragraph, Article 4 of Regulation (EU) No 182/2011 shall apply.'

26. Article 49 is amended as follows:

(a) paragraph 1 is amended as follows:

(i) the introductory wording is replaced by the following:

'1. By 12 September 2028, the Commission shall carry out an evaluation of chapters II, III, IV, V, VI, VII, and VIII and submit a report on its main findings to the European Parliament and to the Council, and to the

PUBLIC

European Economic and Social Committee. That evaluation shall assess, in particular:'

(ia) point (a) is replaced by the following:

~~1b.~~ **(a) situations to be considered to be situations of public emergency for the purpose of Article 15a of this Regulation and the application of Chapter V of this Regulation in practice, in particular the experience in the application of Chapter V of this Regulation by public sector bodies, the Commission, the European Central Bank and Union bodies; the number and outcome of the proceedings brought to the competent authority under Article 18(5) on the application of Chapter V of this Regulation, as reported by the competent authorities; the impact of other obligations laid down in Union or national law for the purposes of complying with requests for access to information; the impact of voluntary data-sharing mechanisms, such as those put in place by data altruism organisations, on meeting the objectives of Chapter V of this Regulation, and the role of personal data in the context of Article 15a of this Regulation, including the evolution of privacy-enhancing technologies;'**

(ii) point (m) is replaced by the following:

'(m) the impact of this Regulation on SMEs and SMCs with regard to their capacity to innovate and to the availability of data processing services for users in the Union and the burden of complying with new obligations'

(b) the following paragraph 2a is inserted:

'2a. By [date = entry into force plus 5 years], the Commission shall carry out an evaluation of chapters VIIa, VIIb and VIIc of this Regulation and submit a report on its main findings to the European Parliament and to the Council as well as to the European Economic and Social Committee.

The report shall assess, in particular:

PUBLIC

(a) the state of registrations of data intermediation services and the type of services they offer;

(b) the type of data altruism organisations registered and an overview of the objectives of general interests for which data are shared in view of establishing clear criteria in that respect.'

(c) the scope and social and economic impact of Chapter VIIc Section 2 including

(d) the extent of the increase in re-use of public sector documents to which Section 2 of Chapter VIIc applies, especially by SMEs and SMCs;

(ii) ~~(e)~~ the impact of the high-value datasets;

(iii) ~~(f)~~ the interaction between data protection rules and re-use possibilities;

(g) Member States shall provide the Commission with the Information necessary for the preparation of that report.'

(c) paragraph **4** ~~5~~ is replaced by the following:

'**4** ~~5~~. On the basis of the reports referred to in paragraphs 1, ~~and~~ 2 and 2a, the Commission may, where appropriate, submit a legislative proposal to the European Parliament and to the Council to amend this Regulation.'

27. Annex I is added as set out in the Annex II to this Regulation.

Article 2

Amendments to Regulation (EU) 2018/1724

In the table in Annex II to Regulation (EU) 2018/1724, the entry 'Starting, running and closing a business' is replaced by the following:

Life events	Procedures	Expected output subject to an assessment of the application by the competent authority in accordance with

		national law, where relevant
Starting, running and closing a business	Notification of business activity, permission for exercising a business activity, changes of business activity and the termination of a business activity not involving insolvency or liquidation procedures, excluding the initial registration of a business activity with the business register and excluding procedures concerning the constitution of or any subsequent filing by companies or firms within the meaning of the second paragraph of Article 54 TFEU	Confirmation of the receipt of notification or change, or of the request for permission for business activity
	Registration of an employer (a natural person) with compulsory pension and insurance schemes	Confirmation of registration or social security registration number
	Registration of employees with compulsory pension and insurance schemes	Confirmation of registration or social security registration number
	Submitting a corporate tax declaration	Confirmation of the receipt of the declaration
	Notification to the social security schemes of the end of contract with an employee, excluding procedures for the collective termination of employee contracts	Confirmation of the receipt of the notification

PUBLIC

	Payment of social contributions for employees	Receipt or other form of confirmation of payment of social contributions for employees
	Registration as a data intermediation services provider	Confirmation of the registration
	Registration as a data altruism organisation recognised in the Union	Confirmation of the registration

PUBLIC

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 **conducted**~~which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out~~ with the aim of contributing to the growth of **society's**~~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**, and producing verifiable and transparent results in an autonomous and independent manner**~~ in the relevant research area. This does not exclude that the research may also aim to further a commercial interest~~.'

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) ~~unintentional and residual~~**incidental** processing **of residual data, where not intended by the controller,** in the context of the development and **technical** 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**~~, including~~ **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** ~~unintentionally~~**incidentally and residually involved** in the datasets used for **the development** ~~oftraining, testing or~~**of** ~~validation~~**and** ~~or~~**technical** ~~in~~**operation of** the AI system or AI model, **including training, validation and testing,** the controller shall **erase**~~remove~~ such data **without undue delay. If erasure**~~. If removal~~ of those data **proves to be technically 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.’

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**, for a request under Article 15, where an abusive intention on the part of**~~also, for requests under Article 15 because~~ the data subject **submitting those requests can be demonstrated,** ~~abuses the rights conferred by this regulation for purposes other than the protection of their data~~, the controller may either:

(a) charge a reasonable fee **proportionate to**~~taking into account~~ 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 ~~that~~ **that** the request is manifestly unfounded or ~~that~~ **that** there are reasonable grounds to believe ~~that~~**, in the light of all the relevant circumstances of the case, that the request is** ~~manifestly unfounded, it is~~ excessive **or that there is an abusive intention on the part of the data subject**.'

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

'5~~4.~~ Paragraphs 1, 2 and 3 shall not apply **if and to the extent that:**

a)~~where the personal data have been collected in the context of a clear and circumscribed relationship between data subjects and a controller exercising an activity that is not data-intensive and~~ there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1~~, unless the controller transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or [or the provision of information would prove impossible]~~**, or**

b) the provision of information would involve a disproportionate effort and the processing is **not** likely to result in a ~~low~~high risk to the rights and freedoms of data subjects **within the meaning of Article 35.**

PUBLIC

This paragraph shall not apply where the processing requires complex processing operations, the processing of large amounts of personal data, [or personal data referred to in Articles 9 and 10.] ~~within the meaning of Article 35~~.'

6. In Article 13, paragraph **6~~5~~** is added:

'6~~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. **The~~A decision which produces legal effects for a~~** data subject **shall have the right not to be subject to a decision~~or similarly significantly affects him or her may be~~** based solely on automated processing, including profiling, **which produces legal effects concerning him or her or similarly significantly affects him or her, unless such processing~~only where that decision~~**:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller **~~regardless of whether the decision could be taken otherwise than by solely automated means~~**;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

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, and 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 to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible to an indefinite number of natural persons without the individual's intervention.

8. Article 33 is amended as follows:

(a) paragraph 1 is replaced by the following:

‘1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 96 hours after having become aware of it, notify the personal data breach **with the support of the national entry**~~via the single-entry~~ point established pursuant to Article **23b**~~23a~~ 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 hours, it shall be accompanied by reasons for the delay.’

(b) the following paragraph is added:

‘1a. Until the establishment of the **national entry**~~single-entry~~ point pursuant to Article **23b**~~23a~~ 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 **establish and make public**~~prepare and transmit to the Commission a proposal for 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 lists**~~. The proposals~~ shall be **available by**~~submitted to the Commission within~~ [OP date = nine months **from the date of**~~of the~~ entry into application of this Regulation]. ~~The Commission after due consideration reviews it, as necessary, and is empowered to adopt it by way of an implementing act in accordance with the examination procedure set out in Article 93(2).~~

7. The **lists**~~template and the list~~ referred to in paragraph 6 shall be reviewed **by the Board** at least every three years and updated where necessary. ~~The Board~~

PUBLIC

~~shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6.~~

8. The Board shall prepare and transmit to the Commission a proposal for a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1. That proposal shall be submitted to the Commission by [OP date = nine months from the date of entry into application of this Regulation]. The Commission after due consideration of the proposal reviews it and is empowered to adopt it by way of an implementing act in accordance with the examination procedure set out in Article 93(2).

9. The template referred to in paragraph 8 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 proposal reviews it and is empowered to adopt any updates by way of an implementing act in accordance with the examination procedure set out in Article 93(2).'

9. Article 35 is amended as follows:

(a) paragraphs 4, 5 and 6 are replaced by the following:

'4. The Board shall **establish and make public**~~prepare and transmit to the Commission a proposal for~~ a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.

5. The Board shall **establish and make public**~~prepare and transmit to the Commission a proposal for~~ a list of the kind of processing operations for which no data protection impact assessment is required.

6. **The lists referred to in paragraphs 4 and 5 shall be published by [OP date = 9 months from the date of entry into application of this Regulation]. These lists shall be reviewed by the**~~The~~ Board **at least every three years**

and updated where necessary~~shall prepare and transmit to the Commission a proposal for a common template and a common methodology for conducting data protection impact assessments~~.'

(b) the following **paragraph is**~~paragraphs are~~ inserted:

'6a. The **Board shall prepare and transmit to the Commission a proposal for a common template and a common methodology for conducting data protection impact assessments.**~~proposals for the lists referred to in paragraphs 4 and 5 and for~~**The**~~the~~ template and methodology ~~referred to in paragraph 6~~ shall be submitted to the Commission **by**~~within~~ [OP date = 9 months **from the date of**~~of the~~ entry into application of this Regulation]. The Commission after due consideration reviews them, as necessary, and is empowered to adopt them by way of an implementing act in accordance with the examination procedure set out in Article 93(2).

6b. ~~The lists and~~ **The**~~the~~ template and methodology referred to in paragraph 6a ~~-~~ shall be reviewed at least every three years and updated where necessary. The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates **by way of an implementing act in accordance with the examination**~~following the~~ procedure **set out in Article 93(2)**~~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 **Board establishes and makes public the lists**~~Commission adopts the implementing act~~ referred to in paragraph **4 and 5**~~6a~~.'

(9a)

10. The following article is added:

'Article **25a - Application of pseudonymisation and identification of a natural person** ~~41a~~

(1) **Controllers and processors may apply~~The Commission may adopt implementing acts to specify means and criteria to determine whether data resulting from~~** pseudonymisation **in order to reduce the risks to the data subjects concerned and to comply with their obligations under this Regulation, in such a manner that the~~no longer constitutes~~** personal data **can no longer be attributed to a specific data subject without the use of additional information~~for certain entities~~. Pseudonymisation shall be subject to appropriate technical and organisational measures to prevent other persons from identifying the data subject.**

(2) Pseudonymised data shall not be considered personal data for ~~a person~~third party if that ~~person~~third party is unable to identify the natural person to whom the data relates~~, unless paragraph 5 applies~~.

(3)~~(2)~~ ~~To determine whether a natural person is identifiable, including through personal data having undergone pseudonymisation, account~~**~~For~~ shall be taken Where a third party discloses, transmits or ~~the purpose of paragraph 1 the Commission shall be taken~~otherwise makes such data available to another third party and, in light of all ~~the~~relevant circumstances, that other third party possesses or can obtain means reasonably likely to** ~~be used, either by the controller or by another person to identify the natural person directly or indirectly. A natural person is not identifiable where the likelihood of identification is insignificant in practice~~ **enable the data subject to be identified, both the transmission of the data to that other third party and the subsequent processing of the data by that other third party is processing of personal data.~~:~~**

(4)~~(a)~~ Where a processor processes personal data on behalf of a controller, that information shall be considered personal data for the processor, and the processor continues to be subject to the obligations applicable under this Regulation.~~assess the state of the art of available techniques;~~

(5)~~(b)~~ ~~Where a~~**To determine whether a natural person** ~~other than the controller discloses, transmits or otherwise makes such data available to a third party and, in light~~ **is identifiable, including through personal data having undergone pseudonymisation, account shall be taken of all** ~~relevant circumstances, the~~

~~third party possesses or can obtain~~**the means reasonably likely to be used either by the controller or by another person** ~~enable the data subject to be identified, both the transmission of the data to this third party and the subsequent processing of the data by this third party is processing of personal~~**develop** ~~data. Criteria and or categories for controllers and recipients~~ to ~~assess~~**identify** the ~~risk of re-identification in~~**natural** ~~relation~~**person** ~~to~~**directly** ~~typical~~**or** ~~recipients~~**indirectly**. ~~of data.~~

(6) 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.

(7) ~~(3)~~The **Chair**~~implementation~~ of the **Board shall request the opinion referred to in paragraph 4 no later than 6 months after the entry into force of this Regulation. The opinion shall be reviewed and updated where necessary** ~~means and criteria outlined in an implementing act may be used as an element to demonstrate that data cannot lead to reidentification of the data subjects~~.

~~(4) The Commission shall closely involve the EDPB in the preparations of the implementing acts. The EPDB shall issue an opinion on the draft implementing acts within a deadline of 8 weeks as of the receipt of the draft from the Commission.~~

~~(5) The Implementing Acts shall be adopted in accordance with the examination procedure referred to in Article 93(3).'~~

11. ~~In~~ Article **57**~~57(1)~~ 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 request 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) **establish**~~prepare and transmit to the Commission a proposal for~~ a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment and for which no data protection impact assessment is required, pursuant to Article 35.

haa establish 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.

(hb) prepare and transmit to the Commission ~~a proposal for~~ a common template and a common methodology for conducting data protection impact assessments, pursuant to Article 35.

(hc) prepare and transmit to the Commission ~~a proposal for~~ a common template for notifying a personal data breach to the competent supervisory authority ~~as well as for a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person~~ pursuant to Article 33**.**

(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 25a.'

15. After Article 88, the following **article is**~~articles are~~ added:

~~'Article 88a~~

~~Processing of personal data in the terminal equipment of natural persons~~

~~(1) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation.~~

~~(2) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1).~~

~~(3) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following:~~

~~(a) carrying out the transmission of an electronic communication over an electronic 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.~~

PUBLIC

~~(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~~

~~Automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons~~

~~(1) Controllers shall ensure that their online interfaces allow data subjects to:~~

~~(a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;~~

~~(b) decline a request for consent and exercise the right to object pursuant to Article 21(2) through automated and machine-readable means.~~

~~(2) Controllers shall respect the choices made by data subjects in accordance with paragraph 1.~~

PUBLIC

~~(3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service.~~

~~(4) The Commission shall, in accordance with Article 10(1) of Regulation (EU) 1025/2012, request one or more European standardisation organisations to draft standards for the interpretation of machine-readable indications of data subjects' choices.~~

~~Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 1.~~

~~(5) Paragraphs 1 and 2 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation].~~

~~(6) Providers of web browsers, which are not SMEs, shall provide the technical means to allow data subjects to give their consent and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to 5 of this Article.~~

~~(7) Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation].~~

Article **88 bis**~~88c~~

Processing in the context of the development and operation of AI

(1) ~~Where~~ **The**~~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 **or of**~~as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or~~ an AI model, ~~such processing~~ may be **carried out for a**~~pursued for~~ legitimate **interest of the controller or a third party in accordance with**~~interests within the meaning of~~ Article 6(1)(f) of **this** 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~~.

(2) Paragraph 1 does not affect the obligation of the controller to choose an~~Any such processing shall be subject to~~ appropriate **lawful ground of**~~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 **set out in Article 6 of this Regulation**~~of their personal data~~.

(3) Regardless of the lawful ground of processing pursuant to Article 6, processing in the context of the development and operation of AI shall be subject to appropriate technical and organisational measures and safeguards to protect the rights and freedoms of the data subject in accordance with this Regulation. '

Article 4

Amendments to Regulation (EU) 2018/1725 (EUDPR)

Regulation (EU) 2018/1725 is amended as follows:

1. Article 3 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) point 25 is replaced by the following:~~

~~'(25) for 'electronic communications networks' the definition of Article 2(1) of Directive (EU) 2018/1972 shall apply;'~~

(c) the following points are added:

~~'(27) 'mobile application' means a mobile application as defined in Article 3(2) of Directive (EU) 2016/2102;~~

~~(28) 'online interface' means an online interface as defined in Article 3(m) of Regulation (EU) 2022/2065;~~

(**27**~~29~~) **'**~~"~~scientific research**'**~~"~~ means any research ~~which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out~~ with the aim of contributing to the growth of **society's**~~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**, and producing verifiable and transparent results conducted in an autonomous and independent manner** ~~in the relevant research area. This does not exclude that the research may also aim to further a commercial interest~~.'

2. Article 4 (1)(b) is replaced by the following:

'(b) 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 13, be considered to be compatible with the initial purposes, independent of the conditions of Article 6 of this Regulation, ('purpose limitation');'

3. Article 10 is amended as follows:

(a) in paragraph 2, the following points are added:

PUBLIC

‘(k) ~~unintentional and residual~~**incidental** processing **of residual data, where not intended intended by the controller,** in the context of the development and **technical** 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 4.~~.~~

(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**.’

(b) the following paragraph 4 is added:

‘4. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid 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** ~~unintentionally~~**incidentally and residually involved** in the datasets used for **the development and technical operation of the AI system or AI model, including** training, testing or validation ~~**or in the AI system or AI model**~~, the controller shall **erase**~~**remove**~~ such data **without undue delay. If erasure**~~**. If removal**~~ of those data **proves to be technically 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.’

4. in Article 14, paragraph 5 is replaced by the following:

‘5. Information provided under Articles 15 and 16 and any communication and any actions taken under Articles 17 to 24 and 35 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**, for a request under Article 17, where an**

abusive intention on the part of~~also, for requests under Article 17 because~~ the data subject **can be demonstrated**~~abuses the rights conferred by this Regulation for purposes other than the protection of their data~~, the controller may refuse to act on the request **and inform the data subject of the reason thereof**. The controller shall bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe ~~that~~**, in light of all the relevant circumstances of the case, that the request is** ~~manifestly unfounded or~~ **excessive** ~~it~~ **or that there** is ~~excessive~~ **an abusive intention on the part of the data subject**.'

5. in Article 15 the new 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 13~~ 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 13**, 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.'

6. in Article 24 **is**~~paragraphs 1 and 2 are~~ replaced by the following:

'1. **The**~~A decision which produces legal effects for a~~ data subject **shall have the right not to be subject to a decision**~~or similarly significantly affects him or her may be~~ based solely on automated processing, including profiling, **which produces legal effects concerning him or her or similarly significantly affects him or her, unless such processing**~~only where that decision~~:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller ~~regardless of whether the decision could be taken otherwise than by solely automated means~~;

(b) is authorised by Union 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 10(1), unless point (a) or (g) of Article 10(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.'

(6a) in Article 27, 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 39(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, and 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 to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the

period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible to an indefinite number of natural persons without the individual's intervention.

(6b) The following Article 30a is added:

30a - Application of pseudonymisation and identification of a natural person

(1) Controllers and processors may apply pseudonymisation in order to reduce the risks to the data subjects concerned and to comply with their obligations under this Regulation, in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. Pseudonymisation shall be subject to appropriate technical and organisational measures to prevent other persons from identifying the data subject.

(2) Pseudonymised data shall not be considered personal data for a ~~person~~third party if that ~~person~~third party is unable to identify the natural person to whom the data relates~~, unless paragraph 5 applies~~.

(3) Where a third party discloses, transmits or otherwise makes such data available to another third party and, in light of all relevant circumstances, that other third party possesses or can obtain means reasonably likely to enable the data subject to be identified, both the transmission of the data to that other third party and the subsequent processing of the data by that other third party is processing of personal data.

(4) Where a processor processes personal data on behalf of a controller, that information shall be considered personal data for the processor, and the processor continues to be subject to the obligations applicable under this Regulation.

(5) To determine whether a natural person is identifiable, including through personal data having undergone pseudonymisation, account shall be taken of all the means reasonably likely to be used, either by the controller or by another person to identify the natural person directly or indirectly. ~~A natural person is not identifiable~~

~~where the likelihood of identification is insignificant in practice.~~

~~(4) Where a processor processes personal data on behalf of a controller, that information shall be considered personal data for the processor, and the processor continues to be subject to the obligations applicable under this Regulation.~~

~~(5) Where a person other than the controller discloses, transmits or otherwise makes such data available to a third party and, in light of all relevant circumstances, the third party possesses or can obtain means reasonably likely to enable the data subject to be identified, both the transmission of the data to this third party and the subsequent processing of the data by this third party is processing of personal data.~~

7. in Article 34, paragraph 1 is replaced by the following

‘1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 96 hours after having become aware of it, notify the personal data breach to the European Data Protection Supervisor. Where the notification to the European Data Protection Supervisor is not made within 96 hours, it shall be accompanied by reasons for the delay.’

~~8.~~ **~~In Article 37 the following paragraphs are added:~~**

~~‘(2) 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.~~

~~(3) 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 law within the meaning of, and subject to the conditions of Article 5, to safeguard the objectives referred to in Article 25(1).~~

~~(4) 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 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**, including its functionality, **explicitly requested by the data subject ;**

(c) Creating**creating aggregated information about the usage of an online service to measure the audience of** that**such a service,** provided that**where it is carried out by the** provider of the**controller of that online service** requested by the subscriber or user, or by a third party on behalf of that provider, and the data collected for the purpose of aggregating the information is not shared with third parties nor combined with data from third parties**solely for its own use;**

(ca) performing audience measurement in compliance with Article 24 of Regulation (EU) 2024/1083, provided that personal data are pseudonymised immediately after collection, and that any information shared with third parties other than those acting either on behalf of or jointly together with that provider does not contain personal data;

(d) **maintaining or restoring the** technical **security of** the means strictly necessary for the provision of an information society**a service provided by the controller and requested by the** subscriber or user or the technical security of**data subject or the terminal equipment used for the provision of such service;.**

(e) measuring the display and performance of advertising that is based solely on the immediate content displayed during an individual visit to a single web page or on the basis of a single search query, provided that such measurement does not involve profiling, data retention or any link with the past or future activity of the subscriber or user, where such measurement is carried out by the provider of an online service, including jointly with others, or by a third party on behalf of that provider

PUBLIC

~~(5) 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 refusesdeclines 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.~~

~~(6) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]]~~

~~(7) 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 a request for consent through automated and machine-readable means.~~

~~(8) Controllers shall respect the choices made by data subjects in accordance with paragraph 7.~~

~~(9) Online interfaces of controllers which are in conformity with harmonised standards or parts thereof referred to in paragraph 4 of Article 88b of Regulation (EC) 2016/679 shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 7.~~

PUBLIC

~~(10) Paragraphs 7 to 9 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation].'~~

9. Article 39 is amended as follows:

(a) ~~Paragraph~~**paragraph** 4 is replaced by the following:

'4. The lists, the template and methodology ~~adopted by the Commission and~~ referred to in ~~paragraph 6a of~~ Article 35 of Regulation (EU) 2016/679 should apply to the processing of personal data under this Regulation.'

(b) Paragraphs 5 and 6 are deleted.

~~10. the following article is added:~~

~~'Article 45a~~

~~The common criteria adopted by the Commission and referred to in article 41a of the Regulation (EU) 2016/679 should apply to the processing of personal data under this Regulation.'~~

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

'3. Member States~~This paragraph~~ shall **ensure that the storing of information, or gaining of access to information already stored, in the terminal equipment of a**~~not apply if the~~ subscriber or user is **only allowed when that**~~a natural~~ person **has given his or her consent, in accordance with Regulation (EU) 2016/679.**

Storing of information, or gaining of access to~~, and the~~ information **already** stored**, in the terminal equipment of a subscriber or user without consent, and subsequent** ~~or accessed constitutes or leads to the~~ processing of personal data **for the same purpose, shall be**

lawful to the extent it is solely related to and strictly necessary for the following purposes:

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

b) providing a service, including its functionality, explicitly requested by the subscriber or user;

c) Creating anonymous aggregated information about the usage of an online service to measure the audience of that service, provided that it is carried out by the provider of the service requested by the subscriber or user, or by a third party on behalf of that provider, and the data collected for the purpose of aggregating the information ~~is not~~are not processed for another purpose, shared with third parties ~~nor~~or combined with data from third parties;

d) performing audience measurement in compliance with Article 24 of Regulation (EU) 2024/1083, provided that personal data are pseudonymised ~~immediately~~ after collection and not processed for another purpose, and that any information shared with third parties other than those acting either on behalf of or jointly together with that provider does not contain personal data;

e) maintaining or restoring the technical security of the means strictly necessary for the provision of ~~an information society~~a service requested by the subscriber or user or the technical security of the terminal equipment used for the provision of such service;

f) measuring the display and performance of advertising that is based solely on the immediate content displayed on a subscriber or user's online interface during an individual visit ~~to a single web page~~ or on the basis of a single search query~~, provided that such measurement~~ and that does not involve ~~profiling, data retention or any link with the past or future activity of the subscriber or user~~ the processing of personal data, where such measurement is carried out by the provider of an online service, including jointly with others, or ~~by a third party~~ on behalf of that provider. Such measurement shall not involve profiling or processing of data relating to the subscriber or user's past or future activity, including activity across sites or services. Data collected for such measurement shall be

pseudonymised after collection and shall not be processed for another purpose.

The subscriber or 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 subscriber or 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 subscriber or user. If the subscriber or user refuses a request for consent, the provider shall not make a new request for consent for the same purpose for a period of at least six months.

2a. In Article 15a, the following paragraph is added:

5. Member States shall designate the competent supervisory authority under Regulation (EU) 2016/679 for the supervision and enforcement of the rules under this Article 5, paragraph 3, of this Directive.

2b. 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].

2c. In Article 18, the following paragraph is added:

The Commission shall submit to the European Parliament and the Council, no later than [XX months after the adoption of this Regulation], a report reviewing and assessing the use of privacy-enhancing technologies, including in relation to the storing of, or gaining access to information on terminal equipment, taking into account the state of the art, and with a view to provide incentives and legal certainty for service providers in deploying such technologies. Where appropriate, the Commission shall submit proposals to update the applicable legal framework, taking account of the results of that report, any sectoral developments and any

other proposal it may deem necessary in order to improve the effectiveness of the rules on the storing of, or gaining access to information on terminal equipment.'

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**~~incident~~ reporting **information point**

(1) ENISA shall develop and maintain **an incident reporting information**~~a single-entry~~ point to support **the identification and fulfilment of** the obligation to report incidents and related events under the Union legal acts where those Union legal acts provide so ('**incident reporting information**~~single-entry~~ point'). ~~Without prejudice to Article 16 of Regulation (EU) 2024/2847 of the European Parliament and of the Council, ENISA may ensure that the single-entry point builds on the single reporting platform established under that Regulation.~~

~~(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~~The incident reporting **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.~~

(2) The incident reporting information point shall:

(a) be designed to allow, on the basis of relevant information provided, the identification of the applicable reporting obligations referred to in paragraph 1 and the direction to the appropriate national entry point referred in Article 23b, and

(c) make available simplified and documented information on incident notification processes in the different Member States.

(3) When developing the incident reporting information point, ENISA shall consult the relevant national competent authorities under the relevant Union legal acts, the Cooperation Group, the CSIRT Network and other relevant bodies or groups established at Union level under relevant Union legal acts. ENISA shall establish structured communication channels to ensure that information available on the incident reporting information point is swiftly and effectively updated. Member States shall communicate to ENISA all relevant and necessary information for the purpose of paragraph 1a.

(4) 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.

(5) After establishing the incident reporting information point and in cooperation with the 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:**~~

PUBLIC

~~(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~~

PUBLIC

~~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.~~

1a. The following Article 23b is added:

~~6b.~~ **'Article 23b**

~~6c.~~ **National entry point for incident reporting**

(1) Member States shall establish and maintain a national entry point supporting and facilitating the reporting of incidents and related events under the Union legal acts where those Union legal acts provide so.

~~2.~~

(2) Member States shall retain flexibility to configure their national entry point in accordance with their existing national 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 endeavour to design their national entry point with a view to making the national entry points interoperable with the national entry points of 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 other relevant bodies or groups established at Union level under relevant Union legal acts provide non-binding recommendations to support Member States in the establishment, maintenance and secure operation of their respective national entry point. Those recommendations shall address technical,

operational and organisational measures, taking into account experiences and lessons learned from existing reporting structures. Those recommendations shall include technical specifications 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.

(5) ENISA shall, by [18 months from the date of entry into force of this amending Regulation], in cooperation with Member States, develop an open-source solution that may be used by Member States in setting up their national entry point in accordance with paragraph 1, with the objective of strengthening interoperability between national systems and enable faster, more effective cross-border data sharing when a situation requires coordinated action

1b. The following article 23c is added :

~~8.~~ **'Article 23c**

~~9.~~ **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 elements and differences in 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.

~~11.~~ **The report shall in particular consider concrete steps and a timeline for further harmonisation efforts on incident reporting under the Union legal acts.**

(3) Building on the report referred in paragraph (1), ENISA shall, in cooperation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts, and other relevant bodies or groups established at Union level under relevant Union legal acts, develop guidelines for further harmonisation on 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.

~~16.~~ **ENISA shall present to the Commission and Council 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.~~

1c. The following article 23d is added :

~~7b.~~ **'Article 23d**

~~7c.~~ **Cross-border incident notification**

~~7d.~~ **(1) Member States should aim at facilitating cross-border notifications between national entry points, where incidents have cross-border impacts.**

~~7e.~~ **(2) ENISA shall, in cooperation with the CSIRTs network, the Cooperation Group and competent authorities under the relevant Union legal acts, as well as with other relevant bodies or groups established at Union level under relevant Union legal acts, harmonise its relevant tools with national incident notification**

PUBLIC

templates and facilitate an automatisation process to exchange information about cross-border impacts.

~~7f.~~ **(3) Member States shall retain control over the scope of information shared and any access to such information. '**

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 **national entry**~~single-entry~~ point ~~established~~ pursuant to Article **23b**~~23a~~.

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 incident reporting 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 **national entry**~~the single-entry~~ point **referred to in**~~established pursuant to~~ Article **23b**~~23a~~, 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 **supported**~~made~~ through the **national entry**~~single-entry~~ point pursuant to Article **23b**~~23a~~ 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 **supported**~~made~~ through the **national entry**~~single-entry~~ point pursuant to Article **23b**~~23a~~ 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 **supported**~~made~~ through the **national entry**~~single-entry~~ point pursuant to Article **23b**~~23a~~ 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 **with the support of the national entry**~~via the single-entry~~ point established pursuant to Article **23b**~~23a~~ 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 **with the support of the national entry**~~via the single-entry~~ point established pursuant to Article **23b**~~23a~~ 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 **with the support of the national entry**~~via the single-entry~~ point established pursuant to Article **23b**~~23a~~ 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~~Repeals~~ **and transitory clauses**

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

~~1a.~~ **Articles 2(11), 2(12), 6, 8 to 10, 12 to 14, 16, 17, and 18 paragraphs (2) to (4), 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.~~

2~~3~~. The following acts are repealed~~, with effect from [Date, aligned with the entry into application of the amendments]~~:

a) **Chapters III, IV, V, VI, VII of** Regulation (EU) 2022/868;

b) Regulation (EU) 2018/1807;

3. Chapter I and II of Regulation (EU) 2022/868 and Directive 2019/1024 are repealed [18 months after the publication in the Official Journal of the European Union].

~~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.

PUBLIC

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.

~~**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. **By way of derogation**~~**Deviating**~~ 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 **national entry**~~**single-entry**~~ point set out in Article **23b**~~**23(4)**~~ 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 **30**~~**24**~~ 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	*For the Council*
The President	*The President*

PUBLIC

ANNEX I

Correlation table

Directive (EU) 2019/1024 (Open Data Directive)	Regulation (EU) 2023/2854 amended by this Regulation (Data Act)
Article 1(1)	32i(1)
Article 1(2)(a)(b)	32i(2)(a)(b)
Article 1(2)(c)	32i(3)(d)
Article 1(2)(d)(i)	32i(2)(c)
Article 1(2)(d)(ii)-(iii)	32i(3)(a)
Article 1(2)(e)	32i(3)(g)
Article 1(2)(f)	32i(3)(b)(i)
Article 1(2)(g)	32i(3)(c)
Article 1(2)(h)	32i(3)(b)(ii)
Article 1(2)(i)	32i(2)(d)
Article 1(2)(j)	32i(3)(d)
Article 1(2)(k)	32i(3)(e)
Article 1(2)(l)	32i(3)(f)
Article 1(3)	32i(5)
Article 1(4)	1(5)
Article 1(5)	32i(6)
Article 1(6)	32i(7)
Article 1(7)	32i(8)
Article 2	2
Article 3	32n
Article 4	~~32o~~**32la**
Article 5	32p

PUBLIC

Article 6 (1-5)	32q(1-5)
Article 6(6)	32q(7)
Article 7(1)	32l(2)
Article 7(2)	32l(3)
Article 7(3)	32m
Article 8	32r
Article 9	32s
Article 10	32t
Article 11	32j
Article 12	32k
Article 13	32u
Article 14	32v
Article 15	45(2)
Article 16	46(1) (2)
Article 17	Repealed
Article 18	49(2a)
Article 19	Repealed
Article 20	Repealed

PUBLIC

Regulation (EU) 2022/868 Data Governance Act	Regulation (EU) 2023/2854 amended by this Regulation (Data Act)
Article 1(1)	1(1)
Article 1(2) first subpraragraph	32i(4)
Article 1(2) second subpraragraph (a)	32i (5)
Article 1(2) second subparagraph (b)	Repealed
Article 1(2) third subpraragraph	1(12)
Article 1(3)	1(5)
Article 1(4)	Repealed
Article 1(5)	1(6) second subpraragraph
Article 3(1)	2(54), 32i(1)(a), 32i(4)(a)
Article 3(2)(a)	32i(4)(b)
Article 3(2)(b)	32i(2)(d)
Article 3(2)(c)	32i(4)(c)
Article 3(2)(d)	32i(2)(c)
Article 3(2)(e)	32i(2)(a)
Article 3(3)(a)	32i(9)
Article 3(3)(b)	32i(5)
Article 4	32k
Article 5 (1), (3) – (6), (8)	32w
Article 5(2)	32j
Article 5(7)	32i(7)
Article 5 (9)- (14)	32x
Article 6	32y

PUBLIC

Article 7	32z
Article 8	32aa
Article 9	~~32ab~~**32la**
Art. 10	Repealed
Art. 11 (1)	32e(1)
Art. 11 (2)	Art. 32e (1)
Art. 11 (3)	Art. 32e (2) in conjunction with Art. 37 (11) Art. 37 (12) Art. 32g (1) Art. 37 (13)
Art. 11 (4)	32e(4)
Art. 11 (5)	32e(4)
Art. 11 (6)	Art. 32e(3)
Art. 11 (7)	Repealed
Art. 11 (8)	Repealed
Art. 11 (9)	Art. 32a (3), (4), (6)
Art. 11 (10)	Art. 32g (4) Art. 32a (2) Art. 32g (5)
Art. 11 (11)	Art. 32g(7)
Art. 11 (12)	Art. 32g(8)
Art. 11 (13)	Art. 32g(8)
Art. 11 (14)	Art. 32g(9)
Art. 12	Art. 32g (partially repealed)
Art. 13 (1)	Art. 32b, 37(1), (7)
Art. 13 (2)	Repealed
Art. 13 (3)	Art. 37(3), (5)(g)
Art. 14 (1)	Art. 32g (1)
Art. 14 (2)	Art. 32g (2)
Art. 14 (3)	Art. 32g(3)

PUBLIC

Art. 14 (4)	Art. 32g(4) Art. 14(a)-(c) Repealed
Art. 14 (5)	Repealed
Art. 14 (6)	32g (5)
Art. 14 (7)	Art. 37 (5) (f) Art. 37(15) Art. 37(16)
Art. 15	Repealed
Art. 16	Repealed
Art. 17 (1)	Art. 32a(1)
Art. 17 (2)	Art. 32a(2), (3), (5)
Art. 18	Art. 32d
Art. 19 (1)	Art. 32e(1), 37 (10)
Art. 19 (2)	Art. 37(10)
Art. 19 (3)	Art. 32d(a), 37(11) Art. 37(13)
Art. 19 (4)	Art. 32e(3)
Art. 19 (5)	Art. 32e(4)
Art. 19 (6)	Art. 32e(4)
Art. 19 (7)	Art. 32e(6), (7)
Art. 20 (1)	Repealed
Art. 20 (2)	Repealed
Art. 21 (1)	Art. 32f (1)
Art. 21 (2)	Art. 32f (2)
Art. 21 (3)	Art. 32f (3)
Art. 21 (4)	Repealed
Art. 21 (5)	Art. 32f (4)
Art. 21 (6)	Art. 32f (5)
Art. 22	Repealed
Art. 23 (1)	Art. 32b, 37(1)

PUBLIC

Art. 23 (2)	Art. 37(7)
Art. 23 (3)	Art. 37(5)(g)
Art. 24 (1)	Art. 32g (1)
Art. 24 (2)	Art. 32g (2)
Art. 24 (3)	Art. 32g(3)
Art. 24 (4)	Art. 32g(4)
Art. 24 (5)	Art. 32g(5)
Art. 24 (6)	Art. 37 (5) (f) Art. 37(15) Art. 37(16)
Art. 25	Art. 32h
Art. 26 (1)	Art. 32b(2)
Art. 26 (2)	Repealed
Art. 26 (3)	Art. 32b(4)
Art. 26 (4)	Art. 32b(5)
Art. 26 (5)	Art. 37(9)
Art. 26 (6)	For MS: Art. 37(5)(f) Art. 37(15) Art. 37(16)
Art. 27 (1)	Art. 38(1)
Art. 27 (2)	Art. 38(2)
Art. 28 (1)	Art. 39(1)
Art. 28 (2)	Art. 39(3)
Art. 28 (3)	Art. 39(2)
Art. 29 (1)	Art. 41a (1), (2), 42
Art 29(2)	Repealed
Art 29(3)	Art 41a(4)
Art. 29(4)	Repealed
Art. 30	Art 42

PUBLIC

Art. 31	Art. 32
Art. 32	Art. 45
Art. 33	Art. 46(1),(1a),(2)
Art. 34	Repealed
Art. 35	Art. 49(2a)
Art. 36	Amends Regulation 2018/1724
Art. 37	Repealed
Art.38	Repealed

PUBLIC

Regulation (EU) 2018/1807 (Free Flow of Non-personal Data Regulation)	Regulation (EU) 2023/2854 amended by this Regulation (Data Act)
Article 1	Repealed
Article 2(1)	Repealed
Article 2(2)	Repealed
Article 2(3) subparagraph 1	Repealed
Article 2(3) subparagraph 2	Art. 1(11)
Article 3(1)	Repealed
Article 3(2)	Repealed
Article 3(3)	Repealed
Article 3(4)	Repealed
Article 3(5)	Art. 2(62)
Article 3(6)	Repealed
Article 3(7)	Repealed
Article 3(8)	Repealed
Article 4(1)	Art. 32h
Article 4(2)	Repealed
Article 4(3)	Repealed
Article 4(4)	Repealed
Article 4(5)	Repealed
Article 5	Repealed
Article 6	Repealed
Article 7	Repealed
Article 8	Repealed
Article 9	Repealed

PUBLIC

Annex II

List of thematic categories of high-value datasets, as referred to in Article 32ab(1) of Regulation (EU) 2023/2854

1. Geospatial
2. Earth observation and environment
3. Meteorological
4. Statistics
5. Companies and company ownership
6. Mobility

PUBLIC