EU governments agree a GDPR position letting AI developers rely on legitimate interest

Source copy kept by wheresthe.ai for the story “EU governments agree a GDPR position letting AI developers rely on legitimate interest” (https://wheresthe.ai/d/eu-council-mandate-digital-omnibus-gdpr-ai-legitimate-interest-2026-10/).

Source: https://data.consilium.europa.eu/doc/document/ST-14756-2026-INIT/en/pdf

Text saved 27 Oct 2026 (the source PDF).

SHA-256 of the saved text: bdf687fda2ebef788068d81afb4f0921e3b8a77119a88df371be3e9ddc4dd93f

Documents the source offers: https://data.consilium.europa.eu/doc/document/ST-14756-2026-INIT/en/pdf

---

Council of the European Union Brussels, 22 October 2026 (OR. en)

14756/26 Interinstitutional File: 2025/0360 (COD)

SIMPL 235 ANTICI 233 DATAPROTECT 345 CYBER 422 TELECOM 498 PROCIV 198 COMPET 1231 MI 1054 CODEC 1945

OUTCOME OF PROCEEDINGS From: General Secretariat of the Council To: Delegations No. prev. doc.: 14532/26 No. Cion doc.: 15698/25 + ADD 1 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) - Mandate for negotiations with the European Parliament

Delegations will find in the Annex the text of the mandate for negotiations with the European Parliament on the above-mentioned file as agreed by the Permanent Representatives Committee at its meeting on 21 October 2026.

Changes compared to the Commission proposal are marked in bold and deletions in strikethrough.

14756/26 1 GIP.B EN 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) 910/20142023/2854 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 Committee1,

Having regard to the opinion of the European Central Bank2,

Having regard to the opinion of the Committee of the Regions3,

Acting in accordance with the ordinary legislative procedure,

Whereas:

1 OJ C […], […], p. […]. 2 OJ C […], […], p. […]. 3 OJ C […], […], p. […].

14756/26 2 ANNEX GIP.B EN (1) In its Communication on a simpler and faster Europe4 , 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

14756/26 3 ANNEX GIP.B EN (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) 2016/6795 and (EU) 2023/28546 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)

14756/26 4 ANNEX GIP.B EN (7) Regulation (EU) 2022/868 of the European Parliament and of the Council7 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 Council8. 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 Council9 on guidance on the processing of personal data in the context of scientific research.

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).

14756/26 5 ANNEX GIP.B EN (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 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.

14756/26 6 ANNEX GIP.B EN (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 datato 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.

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).

14756/26 7 ANNEX GIP.B EN (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 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 an entire third country.

(13) An insufficient protection of trade secrets and the challenges in enforcing them it 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.

14756/26 8 ANNEX GIP.B EN (14) Protecting trade secrets from those vulnerabilities is essential for European industriesbusinesses 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.

(14a) To help businesses in understanding the trade secrets 'handbrake' mechanism, and ensuring that it can be

an effective tool in preserving the confidentiality of trade secrets, the Commission should issue guidelines for data holders to apply the handbrake in practice, giving them necessary legal certainty. In these guidelines, the Commission should in particular provide guidance on how to assess serious economic damage and what data holders need to take into account when examining the enforceability of trade secrets protection in third countries. The guidance should include an assessment of categories of data that are especially sensitive in critical sectors and could, when leaked or when their confidentiality is disclosed, be particularly harmful to the interests of data holders. An example of especially sensitive categories of data could be industrial manufacturing know-how. Critical sectors could include, in particular, those listed in Annex I and Annex II, Number 3, 5a, 5d and 5e, of Directive (EU) 2022/2555).

14756/26 9 ANNEX GIP.B EN (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 underin well-defined, urgent situations, which are unforeseeable and limited in time, reducing the technical, administrative and legal challenges that businessbusinesses 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 Council11 does not 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 in such

11 Regulation (EC) No 223/2009No 223/2009No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008No 1101/2008No 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 322/97No 322/97No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164, ELI: http://data.europa.eu/eli/reg/2009/223/oj).

14756/26 10 ANNEX GIP.B EN situationswhen the production of official statistics is required to respond to or support the recovery from a public emergency. It is also necessary to clarify the compensation regime for situations where microenterprises and small enterprises are required to provide data to addressrespond to 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.

14756/26 11 ANNEX GIP.B EN (17) Certain data processing services, which do not fall within the Infrastructure as a Service (IaaS) delivery model, are 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 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, 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.

14756/26 12 ANNEX GIP.B EN (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.

14756/26 13 ANNEX GIP.B EN (19) Regulation (EU) 2018/1807 of the European Parliament and of the Council12 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’ inwithin 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.

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).

14756/26 14 ANNEX GIP.B EN (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 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 innin 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.

14756/26 15 ANNEX GIP.B EN (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.

14756/26 16 ANNEX GIP.B EN (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.

14756/26 17 ANNEX GIP.B EN 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 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.

14756/26 18 ANNEX GIP.B EN (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 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.

14756/26 19 ANNEX GIP.B EN (25) Start-ups, small enterprises and enterprises that qualify as medium-sized enterprises under Articlepoint 2 of the Annex to Commission Recommendation 2003/361/EC13 and 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 Council14 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.

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). 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).

14756/26 20 ANNEX GIP.B EN (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 datainformation 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 opportunities for smaller businesses and new market entrants to innovate and compete in the digital economy.

14756/26 21 ANNEX GIP.B EN (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 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 40(4) and (5) of that Regulation should be deleted.

14756/26 22 ANNEX GIP.B EN (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.

14756/26 23 ANNEX GIP.B EN (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 Council15. 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.

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)

14756/26 24 ANNEX GIP.B EN (27a) Pseudonymisation is one of the possible 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. 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. It is important that pseudonymised data remains subject to appropriate security measures, taking into account the circumstances of a particular processing, in order to protect from the risk of loss, theft or unauthorised disclosure. 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 code of conducts with regard to the pseudonymisation of personal data. Apart from pseudonymisation, other privacy-enhancing technologies could be applied as appropriate.

14756/26 25 ANNEX GIP.B EN (27b) In light of the interpretation provided in the case law of the Court of Justice of the European Union, it is important to provide further clarity on when a natural person should be considered to be identifiable following the application of pseudonymisation to personal data and the transmission to a third party, as well as when such a third party further discloses, transmits or otherwise makes such data available to 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 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. It is important to recall that, for a controller applying pseudonymisation or a processor processing on behalf of the controller, the data subject remains identifiable and therefore Regulation (EU) 2016/670 applies. Data may become ‘personal’ 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 circumstances, which 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.

14756/26 26 ANNEX GIP.B EN (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 meetsactivities meet the conditions of scientific research for the purpose of this Regulation (EU) 2016/679, account can be taken of elements such as the purpose of the research, the methodological and systematic approach and ethical standards applied in the specific area while conducting the research, and adherence to the principles of transparency, reliability, accountability, oversight, verifiability, and rules for in the specific area. 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 activitiesand 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.

14756/26 27 ANNEX GIP.B EN 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, including small and medium-sized undertakings, (Article 179(2) TFEU) and . 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 should be always of a of high qualityassessed and substantiated by the controller on a case-by-case basis, considering the objective characteristics of the research activity, and should adhere to the principles of principles of reliability, honesty, respect and accountability (verifiability not undermine the obligation to apply appropriate safeguards as provided for in Article 89 of Regulation (EU) 2016/679.

(29) It should be reiterated that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. In such cases it is notshould not be necessary to ascertain on the basis of Article 6(4) of this Regulation (EU) 2016/679 whether the purpose of the further processing is compatible with the purpose for which the personal data are initially collected. Such further processing should be considered compatible, and should be carried out in compliance with the principles and appropriate safeguards laid down in Regulation (EU) 2016/679, in particular Article 89.

14756/26 28 ANNEX GIP.B EN (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.

14756/26 29 ANNEX GIP.B EN (32) The processing of personal data for scientific research purposes and the application of the GDPR's provisions on scientific research are conditional on the adoption of appropriate safeguards for the rights and freedoms of data subjects, pursuant to Article 89(1) GDPR. To that end, the GDPR balances the right to protection of personal data, pursuant to Article 8 CFREU, with the freedom of science, pursuant to Article 13 CFREU. The processing of personal data for the purpose of scientific research therefore pursues acan follow public interest within the meaning of Article 6(1)(e) of Regulation (EU) 2016/679 or be based on Member States and Union law. The processing of personal data for the purpose of scientific research may also be necessary for the purposes of the legitimate interestinterests pursued by a controller or by a third-party within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, provided that such research is not contrary to Union or Member State law. This is without prejudice to the obligation of the controller to ensure that all other conditions of Article 6(1)(f) of Regulation (EU) 2016/679 as well as all other requirements and principles of that Regulation are met.

14756/26 30 ANNEX GIP.B EN (33) The development of certain AI systems and AI models may involve the collection of large amounts of data, includingwhich can include personal data and special categories thereof. Special categories of personal data may incidentally and residually exist in the training, testing or validation data sets or be retained in the AI system or the AI model, although the special categories of personal data are not necessary for the purpose of the processing. and 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 removeerase 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 allowedlimited 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. 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 duringthroughout the entire lifecycle, that is to say during the development and operation, of an AI system or AI model and, once it identifies such data, effectively remove them. If removalerase them. If erasure would prove technically impossible or require manifestly disproportionate effort, notably where the removalerasure 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

14756/26 31 ANNEX GIP.B EN 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 operation 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. It is recalled that Article 6(1)(e) may be regarded as a lawful ground of processing where a public authority develops, including training, or operates an AI system or an AI model used in the performance of a task carried out in a public interest or in the exercise of official authority. 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 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. It is important to clarify that the development and operation of an AI system or AI model does not in itself constitute a legitimate interest, and the applicability of Article 6(1)(f) to processing in the context of AI is to be assessed on a case-by-case basis, taking into account the underlying purpose of that processing.

14756/26 32 ANNEX GIP.B EN (34) Processing of biometric data, as defined in Article 4(14) of Regulation (EU) 2016/679, means processing of certain characteristics of a natural person through a specific technical means and which allows or confirms the unique identification of that person. The notionProcessing of biometric data includescould be carried out for two distinct functions, namely the identification of a natural person or the verification (also called 'authentication') of his or her claimed identity, both of which rely on different technical processes. The identification process is based on a 'one-to-many' search of the data subject's biometric data in a database, while the verification process is based on a 'one-to- one' comparison of biometric data provided by the data subject, who is thereby claiming his or her identity. Derogating from the prohibition to process biometric data under Article 9(1) of the Regulation (EU) 2016/679 should also be allowed where the verification of the claimed identity of the data subject is necessary for a purpose pursued by the controller, and, where applicable, safeguards laid down in Union law or national law adopted in accordance with Article 9(4) of Regulation (EU) 2016/679. 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.

14756/26 33 ANNEX GIP.B EN For the purposes of this Regulation, biometric identification should be understood as the processing of biometric data through comparison against a database intended to determine the identity of a natural person, whereas biometric verification refers to a one-to-one comparison used solely to confirm a claimed identity. This derogation should apply where suitable safeguards apply to enable the data subject to haveensure that the biometric data or the means needed for the verification are under the sole control of the data subject. Sole control means that the data subject can effectively decide when 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 sidedevice of the data subject or are securely stored at the side ofby 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, thatand subject to measures ensuring the overall security of processing is not likely to create significant risks to his or her fundamental rights and freedoms. The controller does not gain knowledge of the, including during the enrolment phase of data subject's biometric data or only for a very limited timeand 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.

14756/26 34 ANNEX GIP.B EN (35) Chapter III of Regulation (EU) 2016/679 sets out rights of the data subject and corresponding obligations of the controller. 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 Regulation already provides that where the request to exercise a right underof the Regulation that the right of access, which is from the outset favourable to data subjects,(EU) 2016/679 is manifestly unfounded or excessive, the controller may either charge a reasonable fee or refuse to act on the request. The controller should not be abused in the sense thatprovide the data subjects abuse them for purposes other than the protection of their datasubject with the reason thereof. A request made under Article 15 of Regulation (EU) 2016/679 is also to be considered excessive where an abusive intention on the part of the data subject submitting those requests can be demonstrated by the controller. For example, such an abuse of the right of accessabusive intention would arise where the data subject intends to cause the controller to refuse an access request, in order to subsequently demand the payment of compensation, potentially under the threat of bringing a claim for damages. Other examples of abuse include situations where data subjects makesubmits excessive use of the right of accessnumbers of identical or largely similar requests with the onlysole intent of causing damage or harm to the controller or when an individual makes. Repeated requests are not automatically excessive in nature but may indicate an abusive intent on the part of the data subject. Other examples of an abusive intention include situations where a data subject submits a request, but at the same time offers to withdraw it in return for some form of benefit from the controller. Moreover, in order to keep their burden to a reasonable extent, controllers should bear a lower burden of proof regarding the excessive character of a request than regarding the manifestly unfounded character of a request. The reason is that the manifestly unfounded character of a request depends on facts that lie principally within the controller's sphere of responsibility, whereas the excessive character of a request concerns the possibly abusive conduct of, when a data subject, submits a request with the sole purpose of obtaining compensation for an alleged infringement which lies primarily outside the controller's sphere of influence, and

14756/26 35 ANNEX GIP.B EN 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) 2016/679is deliberately provoked by the data subject should be as specific as possible. Overly broad and undifferentiated, 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 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.

14756/26 36 ANNEX GIP.B EN (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 thethat Regulation, this derogation should be extended to situations where the processing is not likely to result in a high risk, within the meaning of Article 35 of the Regulation, and there are reasonable grounds to assumebelieve that the data subject already has the information referred to in points (a) and (c) of paragraph 1 of

Article 13 of Regulation (EU) 2016/679, in the light of the context in which the personal data havehas been collected, in particular regarding the relationship between data subjects and the controller. Theseand where the processing is not likely to result in a high risk, within the meaning of Article 35 of that Regulation. This derogation should be the situationsnot apply where the context of theprocessing requires complex processing operations, the processing of large amounts of personal data, or personal data referred to in Articles 9 and 10 of Regulation (EU) 2016/679. For example, there can be reasonable grounds to believe that the data subject already has such information in a direct and clearly circumscribed relationship, established for instance where between the controller and the data subject is very clear and circumscribed and the controller's activity is not data-intensiveinteract directly in a specific occasion, such as the relationship between a craftsman and their clients,.

14756/26 37 ANNEX GIP.B EN 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 nor complex processing operations or the processing of personal data referred to in Articles 9 and 10 of Regulation (EU) 2016/679 and where the scope of processing is limited to the minimum data necessary to perform the service. The controller's activity is not data-intensive where it collects a low amount of personal data and its processing operations are not complex, which is not the case, for example, in the field of employment. In such circumstances, that is to say when the processing is non data-intensive, non-complex and where the controller collects a low amount of personal datacases, 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.

14756/26 38 ANNEX GIP.B EN (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 forthat data subject has the right not to be subject to a decision based solely on automated processing, except when specific conditions are met and in accordance with rules governing the processing of personal data when the data controller makes decisions which have legal effects concerning the data subject or similarly significant effects on the data subject, based solely on automated processing. In order to provide greater legal certainty, it should be clarified that decisionswhen assessing whether a decision based solely on automated processing are allowed when specific conditions are met, as set out in Regulation (EU) 2016/679. It should also be clarified that when assessing whether a decision is necessary for entering into, or performance of, a contract between the data subject and a data controller, as set out in Article 22(2)(a) of Regulation (EU) 2016/679, it should not be required that the decision could be taken only by solely automated processing. This means that The fact that the decision could also be taken by a human does not

prevent the controller from taking the decision by solely automated processing. When several equally effective automated processing solutions exist, the controller should use the less intrusive one.

14756/26 39 ANNEX GIP.B EN (39) In order to reduce the burden on controllers while ensuring that supervisory authorities have access to the relevant information and can act on violations of the Regulation, the threshold for notification of a personal data breach to the supervisory authority under Article 33 of Regulation (EU) 2016/679 should be aligned with that of communication of a personal data breach to the data subject under Article 34 of that Regulation. In the case of a data breach that is not likely to result in a high risk to the rights and freedoms of natural persons, the controller should not be required to notify the competent supervisory authority. The higher threshold for notifying a data breach to the supervisory authority does not affect the obligation of the controller to document the breach in accordance with paragraph 5 of Article 33 of Regulation (EU) 2016/679, or its obligation to be able to demonstrate its compliance with that Regulation, in accordance with Article 5(2) of that Regulation. In order to facilitate compliance by controllers and a harmonised approach in the Union, the Board should prepare a common template for notifying data breaches to the competent supervisory authority andestablish and make public 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 themit, 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.

14756/26 40 ANNEX GIP.B EN (39a) In order to facilitate compliance obligations and the establishment of the contract or other legal act governing the processing by a processor on behalf of the controller, the processor should also be subject to the general obligation of data protection by design and by default under Regulation (EU) 2016/679 to extent it relates to 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.

14756/26 41 ANNEX GIP.B EN (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 preparedestablished and made public by the Board and adopted by the Commission as an implementing act. In establishing the lists, due account should be taken of the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons. In order to facilitate compliance by controllers, the Board should also prepare 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.

14756/26 42 ANNEX GIP.B EN (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, for the purpose of the consistent application of that Regulation, it is recalled that data transfers to a third country or an international organisation where one of the derogations of Article 49(1), points (d) and (f) to (g), of Regulation (EU) 2016/679 applies are not required to be non-repetitive. Thus, for example, the derogation in point (d) allows such data transfers where necessary for important reasons of public interest, including international data exchange between tax administrations, even where those transfers are repetitive, if that is necessary to achieve the public interest at issue.

14756/26 43 ANNEX GIP.B EN (41) Regulation (EU) 2018/1725 of the European Parliament and of the Council16 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 Council17 applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Regulation (EU) 2018/1725 and Directive (EU) 2016/680 should be brough into alignment with the amendments to Regulation (EU) 2016/679 introduced by this Regulation.

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

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, 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).

14756/26 44 ANNEX GIP.B EN (43a) Directive 2002/58/EC on privacy and electronic communications (‘ePrivacy Directive’), last revised in 2009, provides a framework for the protection of the right to privacy, including the confidentiality of communications. It also specifies Regulation (EU) 2016/679 in relation to processing of personal data in the context of electronic communication services. It protects the privacy and the integrity of subscriber’s or user's terminal equipment used for such communications.

(44) The storing of personal datainformation, or the gaining of access to personal datainformation already stored, in a terminal equipment and the subsequent processing of such data should be regulated under a single legal framework, namely Regulation (EU) 2016/679Directive 2002/58/EC on privacy and electronic communications,

where the subscriber of the electronic communications service or the user of the terminal equipment is a natural person. The amendments presented in this Regulationto this Directive should continue to offer the highest levels of protection for personal data, while simplifying the experiences of data subjects in exerting their rights and expressing their choices online. The amendments concern in particular storage of information in that equipment, accessing or otherwise collecting information from that equipment that entails the processing of personal data through cookies or similar technologies to gain information from the terminal equipment. Privacy enhancing technologies that reduce the processing of personal data and support the effective implementation of the obligations of data minimisation and data protection by design and by default 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 technologiesThe relevant rules should also apply regardless of whether the terminal equipment is owned by the natural person or by another legal or natural person.

(44a) The storing of personal datainformation, or the gaining of access to personal datainformation 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.

14756/26 45 ANNEX GIP.B EN (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 the data subjecta subscriber or user, it is necessary to define a limitative list of purposes for which the processing should be permitted without consent. As regards storing of personal datainformation, or the gaining of access to personal datainformation already stored, in a terminal equipment, and subsequent processing that is necessary for those purposes, this Regulationthe Directive should therefore provide that thesuch processing is lawful. The, including when being carried out jointly with or on the behalf of a controller, such as. For example a media service provider, may mandate a processorthird party, such as a market research company, to carry out thesuch 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.

14756/26 46 ANNEX GIP.B EN (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.

(44f) Maintaining or restoring the security of a service provided by a 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 measures, such as security updates, are strictly necessary and proportionate, to maintain or restore the security of the service or terminal equipment, 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 beyond what is strictly necessary and proportionate for that security purpose. 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.

14756/26 47 ANNEX GIP.B EN (44g) 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 the advertisement displayed such as capping cookies and advertising measurement cookies. Such measurement of the display and performance of contextual advertising should be lawful without the consent of the user where it is carried out by the provider of an online service, including jointly with others, or on behalf of that provider, provided 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's past or future activity, including activity across sites, apps or services.

14756/26 48 ANNEX GIP.B EN (44g) For the subsequentfurther processing of personal data for other purposecompatible purposes 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 subsequentfurther 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.

14756/26 49 ANNEX GIP.B EN (45) Data subjectsSubscribers or users that have refused a request for consent are often confronted with a new request to give consent each time they visit the same controllerprovider's online service again. This may have detrimental effects to the data subjectssubscribers or users which may consent just in order to avoid repeating requests. The controllerprovider should therefore be obliged to respect the data subject'ssubscriber or users' 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. The provider may request consent within this period where a new request for consent is necessary, for example if the purpose of processing changes. This could be the case where a new

service is offered or where substantial changes to the service are made. A new request may also be made where the cookie or other technology recording the subscriber or user's choice is no longer valid for reasons beyond the service provider's control, including when the user has deleted the cookies. Furthermore, the amendments to Directive 2002/58/EC should not be understood as setting out conditions relating to the online revenue streams of media services providers.

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

14756/26 50 ANNEX GIP.B EN (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.

14756/26 51 ANNEX GIP.B EN (49) Several horizontal or sectorial Union legal acts require the notification of the same event to different authorities using different technical means and channels. The single- entryestablishment by Member States of a national entry point for incident reporting should allow entities to fulfil reportingsupport and facilitate the fulfilment of 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. Furthermore, the single-entrynational entry point shouldcould give a possibility for entities to retrieve information that they have previously submitted using the single- entrynational 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.

14756/26 52 ANNEX GIP.B EN (50) To ensure the security of the single-entry pointnational entry points in particular and with a view to designing interoperable national entry points, ENISA should takedevelop non-binding recommendations addressing the appropriate and proportionate technical, operational and organisational

measures to manage the risks posed to the security of the single-entryfor Member States to develop, maintain and securely operate their respective national entry point and the information submitted or disseminated via the single-entry point. When assessing the risk, and the appropriateness and proportionality of those measures, ENISA should take into account the sensitivity of information submitted or disseminated pursuant to the relevant Union legal acts. ENISA should consultestablish a cross-sector working group to develop these recommendations in cooperation with CSIRTs and competent authorities under the relevant Union legal acts when drafting, making use of existing cooperation groups and networks of Member States established under these acts, with a view draft the technical, operational and organisational measures necessary to establish, maintain and securely operate the single-entrynational 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.

14756/26 53 ANNEX GIP.B EN (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.

(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.

14756/26 54 ANNEX GIP.B EN (51) Before enabling theIt is important to support the further harmonisation of incident notification of incidents, ENISA should pilot the functioning of the single-entry point which should include a thorough testing of the specificities and requirements for the notifications for the relevant Union legal acts. Basedand reporting, including by working on the results of the piloting, the Commission should assess the proper functioning, reliability, integrity and confidentiality of the single-entry point. The Commission should consult theexchange and interoperability of information regarding incident reporting. For this purpose and in cooperation withhe CSIRTs network and the, the Cooperation Group and competent authorities under the relevant Union legal acts, by making use of existing cooperation groups and networks of Member States established under these acts, when carrying out the assessment. Where the Commission finds that the single-entry point ensures the proper functioning, reliability, integrity and confidentiality, it should publish a notice to that effect in the Official Journal of the European Union. In case the Commission considers that the proper functioning, reliability, integrity and confidentiality is not ensured, ENISA should take all necessary corrective measures, followed by a reassessment by the Commissiondevelop guidelines to foster the harmonisation of incident notifications.

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

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

14756/26 55 ANNEX GIP.B EN (54) Based on Regulation (EU) 2022/2554, the financial sector has been at the forefront in implementing a harmonised, comprehensive and effective framework, including with regard to incident reporting. In order to simplify compliance, it is appropriate to align the incident reporting framework established under Regulation (EU) 2022/2554 with the single-entrynational entry point, while ensuring continuity and stability of the existing reporting framework, and considering that the single-entry point would be operational after it has been assessed that it ensures the proper functioning, reliability, integrity and confidentiality. Further, Regulation (EU) 2022/2554 has introduced standardised reporting templates streamlining the content of reports for major ICT-related incidents for the financial sector. The experience gained from the adoption of these templates provides valuable insights and best practices that should be taken into account when specifying the type of information, the format and the procedure of a notification for the purposes of reporting to the single-entrynational entry point under Directive (EU) 2022/2555, Directive (EU) 2022/2557 or Regulation (EU) 2016/679, where appropriate. For this purpose, the CommissionMember States 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 approach aims to ensure consistency, promote synergies and reduce administrative burden on entities by minimizing the number of data fields that entities are required to complete, thereby facilitating more efficient and streamlined reporting processes.

(55) Under the relevant Union legal acts, certain incident-specific information is to be shared at a subsequent stage between competent authorities to facilitate effective oversight and coordination. Therefore, the single-entry 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.

14756/26 56 ANNEX GIP.B EN (56) To ensure that incident reporting is carried out via the single-entrynational entry point Directive (EU) 2022/2555, Regulation (EU) 2016/679, Regulation (EU) 2022/2554, Regulation (EU) 910/2014, and Directive (EU) 2022/2557 should therefore be amended accordingly. The single-entrynational entry point should start being used for the purpose of reporting under those acts within 1830 months from the entry into force of this Regulation. When the Commission initiates the mechanisms of the notice delayingAny new amendment to other Union legal acts or new proposals for Union legal acts should establish the date of application to 24 months from thewhen national entry into force of the Regulation, the corresponding provisions of Directive (EU) 2022/2555, Regulation (EU) 910/2014, Regulation (EU) 2022/2554 and Directive (EU) 2022/2557point should continue to apply for the purpose of meeting thebe used for reporting obligations laid down in the provisions.incidents or related events.

(57) In the exceptional event that a technical impossibility prevents the submission of incident notifications using the single-entrynational 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 wasand the European Data Protection Board were consulted in accordance with Article 42(1)42 of Regulation (EU) 2018/1725 of the European Parliament and of the Council18, and delivered itstheir joint opinion on [DATE]. The European Data Protection Board was consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725 and delivered an opinion on [DATE]10 February 2026.

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 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).

14756/26 57 ANNEX GIP.B EN (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) 2019/10502019/1150 should be repealeddeleted. 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, as well ason ranking in Article 5, and on differentiated treatment in Article 7, on the internal complaint-handling system in Article 11 of Regulation (EU) 2019/1150 that are cross-referenced by other legal acts, in particular Directive (EU) 2023/2831 on improving working conditions in platform work, and, as well as provisions in Article 15 ensuring enforcement, will temporarily remain in application until the original acts are amended 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 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.

14756/26 58 ANNEX GIP.B EN (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:

14756/26 59 ANNEX GIP.B EN 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.’. ’

14756/26 60 ANNEX GIP.B EN (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, point (g) ispoints (e) and (g) are replaced by the following:

‘(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:

‘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.

14756/26 61 ANNEX GIP.B EN (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.’’

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;

14756/26 62 ANNEX GIP.B EN (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:

‘(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 :

(a) does not have as its main purpose the intermediation of copyright- protected content;

(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;’

(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:

14756/26 63 ANNEX GIP.B EN (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;;’

(d)(e) the following points (38a) and (38b) arepoint (38a) is 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;

14756/26 64 ANNEX GIP.B EN (2) are not jointly procured by several legal persons for exclusive use among them;

(38b38a) ‘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:

(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 (6362) are added:

‘(44) ‘medium-sized enterprise’ means a medium-sized enterprise as defined in Articlepoint 2 of Annex I to Recommendation 2003/361/EC;

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

(46) ‘university’ means aany 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;

14756/26 65 ANNEX GIP.B EN (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 andor results;

(51) ‘re-use’ means the use by natural persons or legal entities ofpersons of data or 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 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;

14756/26 66 ANNEX GIP.B EN (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;

14756/26 67 ANNEX GIP.B EN (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 documentsdata ;

(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;

(6162) ‘pseudonymisation’ means pseudonymisation as referred to under Article 4(5) of Regulation (EU) 2016/679.

14756/26 68 ANNEX GIP.B EN 3. in Article 4, paragraph 6 is replaced by the following:

Trade secrets shall be preserved and do not have to be disclosed, unless the data holder and the user have taken all necessary measures prior to the disclosure to preserve their confidentiality in particular regarding third parties. 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, and shall agree with the user proportionate technical and organisational measures necessary to preserve the confidentiality of the shared data, in particular in relation to third parties, such as model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct.’

33a. in Article 4, paragraph 8 is replaced by the following:

‘8. In exceptional circumstances, Where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the user poses a highsignificant 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, in particular as regards trade secrets representing industrial manufacturing know-how for entities in the sectors referred to in Annex I and Annex II points 3, 5a, 5d and 5e of Directive (EU) 2022/2555), 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

14756/26 69 ANNEX GIP.B EN Data holders who refuse to share data pursuant to this paragraph, itthe 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, the critical economic sectors and the type of data in those critical economic sectors that typically may give rise to serious economic damage when unlawfully disclosed to third parties, and as regards risks for third country disclosure, on the enforceability of

trade secrets protection in third countries, and how to assess the control of economic operators by third-country entities.

4. in Article 5, paragraph 9 is replaced by the following:

Trade secrets shall be preserved and do not have to be disclosed to third parties, unless the disclosure is strictly necessary to fulfil the purpose agreed between the user and the third party and the data holder and the third party have taken all necessary measures prior to the disclosure to preserve their confidentiality in particular regarding other parties. 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, and shall agree with the third party proportionate technical and organisational measures necessary to preserve the confidentiality of the shared data, in particular in relation to other parties, such as model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct.'

14756/26 70 ANNEX GIP.B EN 44a. in Article 5, paragraph 11 is replaced by the following:

'11. In exceptional circumstances, Where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the third party pursuant to paragraph 9 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the third party poses a high risksignificant 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, in particular as regards trade secrets representing industrial manufacturing know-how for entities in the sectors referred to in Annex I and Annex II points 3, 5a, 5d and 5e of Directive (EU) 2022/2555), 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, itthe 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, the critical economic sectors and the type of data in those critical economic sectors that typically may give rise to serious economic damage when unlawfully disclosed to third parties, and as regards risks for third country disclosure, on the enforceability of trade secrets protection in third countries, and how to assess the control of economic operators by third-country entities.

14756/26 71 ANNEX GIP.B EN 4a- In article 10 paragraph 12 is replaced by the following:

'(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:

'(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;

14756/26 72 ANNEX GIP.B EN 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 an exceptionalthe 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 addressrespond to the public emergency, personal data may also be requested and, where possible, made available in pseudonymizedpseudonymised 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, a and the 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 preventprevents it from mitigating or supporting the recovery from a public emergency. Such requests shall not be made to microenterprises and small enterprises.;’’

14756/26 73 ANNEX GIP.B EN 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 to make a for the 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.;

14756/26 74 ANNEX GIP.B EN (iii) Point (i) is replaced by the following:

‘(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:

‘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:

14756/26 75 ANNEX GIP.B EN (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:

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.’

14756/26 76 ANNEX GIP.B EN (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.

14756/26 77 ANNEX GIP.B EN 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 specific taskstatutory duty 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.;'

14756/26 78 ANNEX GIP.B EN 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.

14756/26 79 ANNEX GIP.B EN 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.

14756/26 80 ANNEX GIP.B EN 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:';'

14756/26 81 ANNEX GIP.B EN (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