Council of the European Union
General Secretariat

Brussels, 24 August 2026

WK 13042/2026 INIT

LIMITE

TELECOM
CYBER
COMPET
MI
IA
CODEC

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

MEETING DOCUMENT

From:	General Secretariat of the Council
To:	Working Party on Telecommunications and Information Society
Subject:	EDPS Opinion on the Proposal for a Regulation establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act)

Delegations will find in the annex the above indicated document.

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

Opinion 14/2026

on the Proposal for a Regulation establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act)

edps.europa.eu

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation 2018/1725 'With respect to the processing of personal data... for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies', and under Article 52(3)'... for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'.

Wojciech Rafał Wiewiórowski was appointed as Supervisor on 5 December 2019 for a term of five years. The selection procedure for a new EDPS mandate for a term of five years is still ongoing.

*Under **Article 42(1)** of Regulation 2018/1725, the Commission shall 'following the adoption of proposals for a legislative act, of recommendations or of proposals to the Council pursuant to Article 218 TFEU or when preparing delegated acts or implementing acts, consult the EDPS where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data'.*

This Opinion relates to the Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act). This Opinion does not preclude any future additional comments or recommendations by the EDPS, in particular if further issues are identified or new information becomes available. Furthermore, this Opinion is without prejudice to any future action that may be taken by the EDPS in the exercise of his powers pursuant to Regulation (EU) 2018/1725. This Opinion is limited to the provisions of the Proposal that are relevant from a data protection perspective.

Executive Summary

On 3 June 2026, the European Commission issued a Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's cloud and AI ecosystem ("Cloud and AI Development Act").

Cloud computing and AI infrastructures have become increasingly important for public administrations, businesses and society. Dependence on a limited number of third-country providers, vendor lock-in, access by third-country authorities and operational discontinuity may also have implications for the rights to privacy and the protection of personal data. The EDPS therefore strongly supports the objectives of the Proposal, i.e. to strengthen the Union's cloud and AI ecosystem, reduce dependencies, increase operational resilience and sovereignty.

Where cloud computing services are used for the processing of personal data, compliance with EU data protection law should serve as the starting point. The Union assurance framework may usefully add specific requirements relating to sovereignty, operational autonomy, resilience, public order, third-country access risks and service continuity. However, those requirements should build upon EU data protection law in order to avoid unnecessary duplication and legal uncertainty. To achieve this objective, the Proposal should further develop:

- the relationship between the Union assurance criteria and audit evidence requirements in Annex II and Annex III and the requirements of EU data protection law;

- the interaction between the data localisation requirements in Annex II and Chapter V of the GDPR and of the EUDPR; and

- the relationship between the associated third-country mechanism under Article 18 of the Proposal and adequacy decisions under Article 45 GDPR.

The EDPS considers that audits, audit evidence and the central repository should be subject to appropriate safeguards, including purpose limitation, confidentiality, security, retention limits and data minimisation. In the spirit of simplification, the EDPS recommends that the methodology and templates to be adopted under Article 29 of the Proposal be designed as an integrated risk assessment framework in order to reduce administrative burden on public administrations. Where appropriate, factual analyses and documentation produced under EU data protection law may support the Article 29 assessment, without affecting the obligations of controllers and processors, or competences of independent supervisory authorities under EU data protection law.

As regards public procurement, the EuroCloud Federation and Commission-led procurement, the EDPS recommends ensuring that the relevant procurement and contractual arrangements enable Union entities, public sector bodies and contracting authorities to comply with their obligations under EU data protection law. The EDPS also provides recommendations to help ensure that measures supporting AI deployment, national cloud and AI strategies, data centre acceleration zones, open-source solutions and edge-related concepts remain consistent with EU data protection law and AI Act. Finally, EDPS also recommends strengthening cooperation between the competent authorities designated under the Proposal, data protection supervisory authorities and, where relevant, cybersecurity authorities and authorities involved in the AI Act governance framework.

Contents

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, Having regard to 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 ('EUDPR')2, and in particular Article 42(1) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction

1. On 3 June 2026, the European Commission issued the Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's cloud and AI ecosystem ("Cloud and AI Development Act" or "the Proposal").

2. The objective of the Proposal is to address the limited and geographically concentrated availability of computing capacity in the Union and the risks associated with dependence on cloud and AI supplied by non-European providers. To that end, it aims to increase computing capacity and AI developed and deployed in the Union, support the deployment of sustainable and innovative computing capacity, address concerns regarding data sovereignty and operational continuity of cloud and AI, and make the supply of cloud computing services more resilient, in particular in the public sector[1].

3. The Proposal pursues these objectives through several sets of measures. In particular, it establishes Cloud and AI Leadership Initiatives, measures on data centre capacity, a Union cloud computing sovereignty framework based on four Union assurance levels, recognition and assessment procedures for cloud computing services, risk assessments by Member States and Union entities, procurement obligations, the European public sector cloud federation ("EuroCloud Federation"), Commission-led procurement activities and measures concerning open-source solutions and software reuse.

4. The present Opinion of the EDPS is issued in response to a consultation by the European Commission of 3 June 2026, pursuant to Article 42(1) EUDPR. The EDPS recommends including a reference to the date of this Opinion in recital (88) of the Proposal.

[1] COM(2026) 502 final, p. 2

2. General Remarks

5. Cloud computing and AI infrastructures have become increasingly important for public administrations, businesses and society. Dependence on a limited number of third-country providers, vendor lock-in, access by third-country authorities and operational discontinuity may also have implications for the rights to privacy and the protection of personal data. The EDPS therefore strongly supports the objectives of the Proposal, i.e. to strengthen the Union's cloud and AI ecosystem, reduce dependencies, increase operational resilience and sovereignty.

6. At the same time, the EDPS notes that data protection is not the primary aim of the Proposal. It pursues internal market, industrial policy, public procurement and digital sovereignty objectives. Nevertheless, several mechanisms introduced by the Proposal may entail or affect the processing of personal data. This is particularly the case for recognition procedures, conformity self-assessments, audits, audit evidence, central repositories, transparency obligations, risk assessments, procurement procedures, Commission-led procurement, the EuroCloud Federation and AI deployment measures. In addition, the EDPS notes that the Proposal aim to promote initiatives that support access to data for AI development, testing and validation, secure large-scale data pooling, the sharing and reuse of training data and AI models across Union public services, and privacy-enhancing health data reuse for AI models and tools.

7. While many provisions of the Proposal specifically concern Union entities and public sector bodies, the Proposal is not limited to them. In particular, private entities operating in sectors of high criticality may also be required to carry out assessments similar to those provided for in Article 29 of the Proposal. The recitals of the Proposal already usefully make reference to certain obligations under Regulation (EU) 2016/679[2]. However, no reference is made to either Regulation (EU) 2018/1725[3] or Directive (EU) 2016/680[4]. As the Proposal explicitly covers Union entities, it should be clarified that any processing of personal data by those entities is subject to Regulation (EU) 2018/1725, and that the EDPS is the supervisory authority competent for personal data processing operations carried out by Union institutions, bodies, offices and agencies. Since the Proposal may also concern cloud services used in areas such as internal security, external border management, criminal justice and law enforcement, reference should also be made, as regards Member States, to Directive (EU) 2016/680.

8. Against this background, the EDPS recommends inserting a dedicated recital recalling the relevant instruments of EU data protection law applicable to the processing of personal data carried out in the context of the Proposal, namely Regulation (EU) 2016/679 ('GDPR'), Regulation (EU) 2018/1725 ('EUDPR'), Directive (EU) 2016/680 ('LED').

[2] 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.
[3] 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.
[4] 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.

3. Building upon EU data protection law

9. Where cloud computing services are used for the processing of personal data, compliance with EU data protection law should serve as the starting point. The Proposal may usefully add specific requirements relating to sovereignty, operational autonomy, resilience, public order, third-country access risks and service continuity. However, those requirements should build on, and remain coherent with, the GDPR, the EUDPR and, where applicable, the LED.

10. The EDPS considers that Union assurance levels should not be designed, assessed or recognised without taking into account the risks that the relevant cloud computing service may pose where personal data is processed. The Proposal itself appears to establish such a link, in particular where Article 29(2) refers to the nature, scope, context and purpose of the processing of personal data and to risks to the rights and freedoms of data subjects. This link is also reflected in several criteria of Annex II concerning, among other elements, subcontracting, outsourcing, data location, access to data, security measures and third-country access.

11. Compliance with EU data protection law will often be instrumental for the application of the Proposal, for example where risk assessments, audit evidence, procurement decisions or recognition procedures rely on findings or documentation already produced for the purpose of complying with EU data protection law. The EDPS there considers that the relationship between the Proposal and EU data protection law should not be limited to the delineation of separate regimes. The Proposal offers an opportunity for genuine simplification and synergies. For this a clear distinction should remain between the *factual elements* of assessments — the establishment of data locations, data flows, subcontracting chains, access arrangements and applicable third-country laws and practices — which can be shared across legal frameworks, and the *normative conclusions* drawn from those elements, which must remain specific to each framework and to the authorities competent under it.

12. In other words, the EDPS considers that the Union assurance framework should be designed as a complementary mechanism, and not as an additional parallel compliance layer. If the Proposal would create parallel or partially overlapping assessments, audit or recognition mechanisms without clearly defining their relationship with EU data protection law, this may increase legal uncertainty and compliance burdens. The EDPS therefore recommends ensuring coherence with existing Union legal frameworks, including by allowing, where appropriate, the use of and reliance on existing assessments, evidence and audit results under EU data protection law, while preserving the distinct obligations of controllers and processors, as well the supervisory competences under the GDPR, EUDPR and LED.

13. To be clear, recognition under a Union assurance level, positive audit opinions, audit reports, audit evidence or compliance with the Proposal should not be understood as replacing the distinct obligations of controllers and processors under EU data protection law or the tasks and powers of data protection authorities and the EDPS. The EDPS therefore recommends explicitly clarifying in a Recital that recognition under a Union assurance level does not amount to a recognition of compliance with the GDPR, EUDPR or LED A cloud computing service recognised as “Union-assured”, “trusted” or “sovereign” is not automatically compliant with EU data protection law. Similarly, audit reports, positive audit opinions, audit evidence and recognition decisions under the Proposal may be relevant elements for controllers and processors when documenting their assessment of cloud computing services, including in relation to security, resilience, subcontracting, access arrangements or third-country risks.

However, they should not be equated to a certification, approval or finding of compliance under EU data protection law.

14. The EDPS further recommends clarifying in a Recital that findings by auditing organisations or competent authorities under the Proposal are without prejudice to findings by data protection supervisory authorities and the EDPS. Conversely, where data protection supervisory authorities or the EDPS have identified serious or systemic issues concerning a cloud computing service provider, such findings should be capable of being taken into account by competent authorities under the Proposal when assessing, reviewing, amending or revoking recognition under a Union assurance level.

15. Finally, the EDPS considers that the interaction between the Proposal and EU data protection law should also be reflected in the governance arrangements established by the Proposal. This is particularly relevant where competent authorities under the Proposal assess, recognise, amend, suspend or revoke a Union assurance level, or where they rely on audits, audit evidence, repository information, transparency notifications or risk assessments that may concern the processing of personal data[5].

4. Union cloud sovereignty framework

4.1. Union assurance levels, recognition and self-assessment

16. Article 16 of the Proposal establishes a Union cloud computing sovereignty framework based on four Union assurance levels. The criteria for those assurance levels are set out in Annex II and apply to cloud computing services provided to Union entities and public-sector bodies.

17. Article 17 of the Proposal refers to the "competent authority of establishment". The EDPS recommends clarifying this concept, in particular where a cloud computing service provider is established in several Member States. In this respect, the Proposal should specify whether the concept is intended to refer to the main establishment of the cloud computing service provider as defined by Article 25(4) or to another connecting factor.

18. In relation to Union assurance level 1, the EDPS notes that Article 19 of the Proposal allows cloud computing service providers to carry out a conformity self-assessment and issue an EU statement of conformity. The EDPS understands that such a mechanism may be appropriate for the lowest Union assurance level. However, given that the EU statement of conformity must be made publicly available and is linked to the recognition mechanism under Article 17, the Proposal should provide that the statement should explicitly mention its scope, *i.e.* that the provider declares compliance with the criteria for Union assurance level 1 set out in Annex II, without prejudice to any assessment of compliance with other elements of the EU legal framework, including with EU data protection law.

[5] The related recommendations on competent authorities, cooperation and enforcement are further developed in Section 4.8 below.

4.2. Criteria for Union assurance levels and audit evidence

19. Annex II and Annex III set out Union assurance criteria and audit evidence requirements which, where cloud computing services are used for the processing of personal data, may be relevant for controllers and processors when documenting aspects of their compliance with the GDPR and the EUDPR[6]. This is particularly the case as regards security of processing, subcontracting and sub-outsourcing, access arrangements, data location, logging, resilience and third-country access risks. However, this requires the relationship between the Union assurance framework and EU data protection law to be clearly articulated, so that such criteria and evidence can be used as supporting elements without being understood as a separate or alternative GDPR or EUDPR conformity assessment or as replacing the accountability obligations of controllers and processors.

20. In addition, the EDPS recommends clarifying certain Annex II criteria that may be particularly relevant for controllers and processors when assessing cloud computing services. First, as regards Annex II, point 1.1(f), the Proposal should clarify what constitutes 'full transparency' around the use of subcontractors, taking into account that subcontracting chains in cloud computing services may be long and dynamic. Appropriate transparency measures could include, for instance, regularly updated subcontractor information, customer notifications of relevant changes and clear information on the role and location of subcontractors involved in the provision of the service[7]. Second, as regards the requirement for Union assurance levels 2, 3 and 4 that the audited provider demonstrate compliance with the "highest cybersecurity standards under applicable Union law", the Proposal should clarify how the applicable standard is to be identified in practice where no Union or national cybersecurity certification schemes exist, preferably by referring to relevant Union legal instruments or recognised technical standards. Third, as regards the restriction on the use of data generated by using the audited service to train or fine-tune AI systems operated by a third country or by a legal entity established in a third country, the Proposal should clarify whether the same restriction also covers the use of such data to test, verify or validate such AI systems, as such use may raise comparable risks.

21. In the same vein, the EDPS recommends, as a matter of legislative technique, that where Annex II and Annex III address matters that are regulated under EU data protection law — such as processor and sub-processor arrangements, data location, access to data or transfers of personal data — they employ the concepts and terminology of the GDPR and the EUDPR, by cross-reference where appropriate, rather than introducing notions that are close but not identical. The use of divergent wording for similar underlying requirements would generate divergent interpretations, additional compliance burdens and legal uncertainty.

---

[6] For example, Annex II refers to subcontracting arrangements, measures to prevent access by third countries or by legal entities established in third countries, and restrictions on the use of data generated by using the audited service for the training or fine-tuning of AI systems operated by such entities. Annex III refers, among other elements, to audit evidence such as contractual clauses, data processing agreements, data flow diagrams, access logs, privileged access records, support access policies and data lineage documentation.

[7] See Article 28(2) and (4) GDPR. See also EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, 7 July 2021, paras 152, 154 and 156-158, according to which, in order for the controller to assess and decide whether to authorise sub-processing, the processor should provide a list of intended sub-processors, including their locations, the activities they will perform and the safeguards implemented; the list of approved sub-processors should be kept up to date; and, in case of general authorisation, the processor should inform the controller in due time of any intended addition or replacement of sub-processors so as to give the controller the opportunity to object.

22. The EDPS also recommends clarifying the extent to which a recognised cloud computing service provider may outsource or sub-outsource all or part of the activities relevant to the provision of the recognised service. This is particularly important in light of Annex II, point 1.1(d), which allows technical and operational support or assistance, including subsequent sub-outsourcing arrangements, to be outsourced to third-party service providers outside the Union where legal, technical and organisational measures are implemented.

23. Finally, the EDPS also invites the co-legislators to address several technical inconsistencies in Annex II which are also relevant from a data protection perspective. First, point 3.1(g) of Annex II refers to an implementing act adopted 'under Article 19', whereas the mechanism for associated third countries is laid down in Article 18 of the Proposal; the cross-reference should be corrected. Second, the data localisation criterion for Union assurance level 4 (point 4.1(c) of Annex II) applies only to customer data 'identified as sensitive' following a risk assessment, whereas the corresponding criteria for levels 2 and 3 cover all customer data. As a result, the highest assurance level appears, as regards data localisation, narrower than the levels below it. Third, the condition that data generated by using the audited service 'are not transferred outside the Union in any case' (criterion (f)) should be reconciled with the possibility for the public sector body to 'explicitly require otherwise' under criterion (c) and, where personal data are concerned, with Chapter V of the GDPR and of the EUDPR.

4.3. Data localisation, third country access and international transfers of personal data

24. The EDPS acknowledges that data localisation in the Union may in some cases be a relevant element for ensuring sovereignty, operational autonomy and limiting exposure to third-country risks. However, data localisation within the Union should not be seen, in itself, as sufficient per se to fully exclude risks of access from third countries. Such risks may also depend on factors such as remote access, support administration, maintenance, monitoring and incident response activities, privileged access management, sub-processing, sub-outsourcing, corporate control, applicable third-country laws, encryption and key management, software dependencies, telemetry, logging, access rights and other technical and organisational measures.

25. The EDPS notes that several criteria in Annex II require customer data, including metadata and telemetry data, to remain exclusively within the Union — in certain cases 'in any case' (criterion (f) for levels 2 to 4), in others unless the public sector body explicitly requires otherwise (criterion (c) for levels 1 to 3). Where such data are personal data, these localisation requirements interact directly with the rules on transfers of personal data to third countries and international organisations under Chapter V of the GDPR and Chapter V of the EUDPR. The Proposal does not address this interaction.

26. This silence leaves a central question unanswered: whether a cloud computing service provider providing a recognised service, or a public sector body or Union entity using it, may transfer personal data covered by the localisation requirements to a third country on the basis of appropriate safeguards within the meaning of Article 46 GDPR or Article 48 EUDPR, such as standard contractual clauses, or on the basis of a derogation within the meaning of Article 49 GDPR or Article 50 EUDPR. As currently drafted, Annex II appears to exclude such transfers, while Chapter V of the GDPR and of the EUDPR, which the Proposal leaves untouched, would permit them where a valid transfer instrument is in place. In the absence of an express articulation, providers, customers, competent authorities and data protection supervisory authorities are likely to resolve this conflict inconsistently, to the detriment of legal certainty.

27. The EDPS recommends that the Union legislator resolve this interaction by expressly anchoring the personal data dimension of the localisation requirements in Article 49(5) GDPR and Article 50(5) EUDPR. Pursuant to those provisions, '*in the absence of an adequacy decision, Union law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation*'. Several Member States have already made use of the corresponding possibility under Article 49(5) GDPR in their national law. The Proposal should provide that, to the extent that data required to remain within the Union constitute personal data, the localisation requirements of Annex II, read in conjunction with the risk assessments under Article 29 and the procurement obligations under Article 30, constitute limits to the transfer of specific categories of personal data expressly set by Union law for important reasons of public interest within the meaning of those provisions. As a consequence, where those limits apply, transfers of the personal data concerned could not be carried out on the basis of appropriate safeguards under Article 46 GDPR or Article 48 EUDPR, nor on the basis of the derogations under Article 49(1) GDPR or Article 50(1) EUDPR.

28. Since Article 49(5) GDPR and Article 50(5) EUDPR refer to specific categories of personal data, those categories should be clearly delimited. In the view of the EDPS, they could be defined as the personal data processed in the context of the public sector activities identified pursuant to Article 29 as requiring Union assurance level 2, 3 or 4 and, at level 4, the data identified as sensitive by the risk assessment. The EDPS considers that those categories should in any event include special categories of personal data (Article 9 GDPR and 10 EUDPR), personal data relating to criminal convictions and offences (Article 10 GDPR and 11 EUDPR) and personal data processed in the context of high-risk processing operations within the meaning of Article 35 GDPR and Article 39 EUDPR. The EDPS also notes that, pursuant to Article 50(6) EUDPR, Union institutions and bodies are required to inform the EDPS of the categories of cases in which Article 50 EUDPR has been applied, which would provide a proportionate transparency mechanism over transfers of personal data in the context of cloud computing services procured by Union entities.

29. The EDPS underlines two consequences of this approach. First, Article 49(5) GDPR and Article 50(5) EUDPR can only apply in the absence of an adequacy decision. Limits set on such bases therefore cannot restrict transfers to third countries covered by an adequacy decision. This is structurally coherent with Article 18 of the Proposal. It also means that, for the highest protection needs — those activities for which absolute localisation is intended under Union assurance levels 3 and 4 — the localisation requirement should remain framed as a procurement and eligibility conditions under the Proposal, since the limits under Article 49(5) GDPR and Article 50(5) EUDPR could not apply to transfers to adequate jurisdictions. Second, the Proposal should expressly clarify, possibly by way of a recital, that the provision gives effect to the possibility envisaged in Article 49(5) GDPR and Article 50(5) EUDPR.

30. Should the Union legislator not follow this recommendation, the EDPS recommends, at a minimum, inserting a provision clarifying that nothing in the Proposal authorises (or exempts from the requirements of) transfers of personal data under Chapter V of the GDPR and of the EUDPR, and that a public sector body or Union entity may 'explicitly require otherwise' within the meaning of Annex II, as regards personal data, only where a valid transfer instrument under Chapter V GDPR or EUDPR is in place and documented. The customer-approved carve-outs in Annex II should not be read as self-standing authorisations for transfers of personal data.

4.4. Associated third countries and adequacy decisions

31. Article 18 of the Proposal provides for a mechanism allowing the Commission to identify associated third countries whose controlled cloud computing service providers may be audited against the criteria for Union assurance level 3, where the conditions set out in that provision are met. The EDPS welcomes that Article 18(a) of the Proposal expressly refers to the existence of an adequacy decision under Article 45 GDPR as one of the cumulative criteria for the purposes of Union assurance level 3. This constitutes a useful articulation between the Proposal and EU data protection law. It confirms that, where personal data are concerned, compliance with the relevant data protection framework is a necessary starting point.

32. The EDPS notes that the assessment to be carried out by the Commission under Article 18 is to a large extent closely related to the assessment underpinning adequacy decisions under Article 45 GDPR and Article 47 EUDPR[8]. The EDPS therefore recommends that assessments under Article 18 formally draw on the findings underpinning the relevant adequacy decision and on the opinions of the EDPB; that the monitoring of implementing acts adopted under Article 18 be aligned with the ongoing monitoring of adequacy decisions under Article 45(4) GDPR, so that relevant developments identified in one framework trigger review in the other.

33. Article 18(3) of the Proposal already provides that the Commission shall publish on its website a list of third countries that fulfil the requirements under Article 18(1) and those that no longer do so. In addition to a list of countries, the Commission's assessments of third-country law and practice should be published in a form that allows controllers, processors and Union entities to rely on them as an authoritative common reference. Such a common reference would substantially reduce duplication of effort across the Union, in particular for small and medium-sized enterprises and smaller Union entities.

34. More specifically, the EDPS recommends that the Proposal expressly regulate the consequences, for implementing acts adopted pursuant to Article 18 and for recognitions granted on their basis, of the suspension, repeal, amendment or invalidation of the underlying adequacy decision, including an obligation to review the implementing act without delay and appropriate transition arrangements for cloud computing services already procured at Union assurance level 3.

35. The EDPS considers that the interaction between Article 17, Article 18 and the relevant Annex II criteria should be further clarified. In particular, the Proposal should make clear how the associated third-country mechanism under Article 18 applies where a cloud computing service provider is established in the Union but is subject to the control of a third country or of a legal entity established in a third country or may be exposed to third-country laws with extraterritorial effects. Such clarification would help ensure legal certainty for providers, public-sector customers and competent authorities applying the Union assurance framework.

36. The EDPS also recommends clarifying the effects of the absence of recognition under Article 18 of the Proposal on the use of cloud computing service providers in third countries that benefit from an adequacy decision under Article 45 GDPR. In particular, the Proposal should

[8] See Adequacy Referential adopted by the Article 29 Working Party adopted 6 February 2018, WP 254 rev1 ; see also See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on 18 June 2001

clarify whether, in the absence of recognition under Article 18, entities in the Union would be prevented, for the purposes of this Regulation, from relying on cloud computing service providers in that third country, even where transfers of personal data to that country would be permitted under Chapter V GDPR.

37. The EDPS further notes that Annex II refers in several places[9] to providers or entities being subject to the control of a third country or of a legal entity established in a third country. The EDPS recommends clarifying whether, and under what conditions, a company established in the Union but controlled by a parent company established in a third country is to be considered subject to such control for the purposes of the Proposal.

4.5. Audits, audit evidence central repository and transparency obligations

38. Article 20 of the Proposal requires cloud computing service providers seeking recognition under Union assurance levels 2, 3 or 4 to undergo independent third-party audits in order to obtain an audit report and an audit opinion from an auditing organisation. Article 21 and Annex III further specify the audit evidence to be assessed in that context.

39. The EDPS considers that audit reports, positive audit opinions and audit evidence under the Proposal may also be relevant elements for controllers and processors when documenting their assessment of cloud computing services under the relevant data protection framework.

40. The EDPS further notes that the audit procedure may involve the processing or disclosure of information that is personal, confidential, commercially sensitive or security-sensitive. This may include, depending on the circumstances, customer data, metadata, telemetry data, logs, access records, information relating to public-sector users, information concerning provider representatives or personnel, subcontractor information, security documentation, data flow diagrams, support access policies, data lineage documentation and other technical or organisational evidence.

41. The EDPS welcomes that Article 20(3) of the Proposal provides for a confidentiality and professional secrecy obligation in respect of information obtained by auditing organisations in the context of audits. At the same time, given that audit evidence may, depending on the circumstances, include personal data or security-sensitive information, the EDPS recommends clarifying that such evidence should be collected, used and shared only for the purposes of assessing compliance with the Union assurance criteria and preparing, reviewing, amending or revoking the relevant audit report and audit opinion. The EDPS also recommends specifying appropriate retention periods.

42. In this respect, the EDPS notes that Annex III requires, as audit evidence for the verification of the Union citizenship of personnel (criterion D), valid official government-issued documents

[9] For example, Annex II, point 2.1(g), refers to the case where the audited provider and the subcontractors involved in the provision of the audited service are subject to the control of a third country or of a legal entity established in a third country. Annex II, point 3.1(g), requires that the audited provider and the subcontractors involved in the provision of the audited service are not subject to such control, subject to the associated third-country mechanism. Annex II, points 2.1(i)(iii), 3.1(i)(iii) and 4.1(i)(iii), also refer to cases where the cloud computing service provider is subject to the control of a third country or of a legal entity established in a third country.

such as passports and national identity cards, as well as personnel lists, payroll records and timesheets. The audit procedure will therefore entail the processing of significant volumes of personal data of the personnel of the audited provider and of its subcontractors. The EDPS recommends that the Proposal expressly require that such processing comply with the principle of data minimisation and be limited to what is strictly necessary for the purposes of the audit. In particular, the verification of citizenship should rely on a documented attestation, i.e. a written confirmation that the citizenship requirement has been verified on the basis of appropriate identity documents, rather than on the collection and retention of copies of identity documents, and the respective roles and responsibilities of the audited provider and of the auditing organisation, as well as appropriate retention limits, should be defined.

43. The EDPS further notes that Annex III, criterion C, lists among the audit evidence 'contracts with the subcontractors that demonstrate compliance with Regulation (EU) 2016/679'. The EDPS recommends reframing this element so that auditing organisations verify the existence and the factual content of the required contracts — such as data locations, data flows and subcontracting chains — without *assessing* or *certifying* their conformity with the GDPR or the EUDPR, which remains a matter for controllers, processors and, ultimately, the competent data protection supervisory authorities and the courts.

44. The EDPS further notes that Article 22 provides for a central repository of recognised cloud computing services, which is to be publicly available and regularly updated. The Proposal should clarify which categories of information will be included in the public part of the central repository and which information, if any, will be accessible only to public sector customers, auditing organisations, competent authorities and the Commission. This clarification is particularly important because audit reports and related evidence may contain personal data, commercially sensitive information or security-sensitive information.

45. In particular, where information relating to the personnel of the audited provider or its subcontractors is processed for the purposes of the audit, the Proposal should clarify what is meant by "staff with operational responsibilities"[10] and what types of "relevant details" may be included. The EDPS recommends ensuring that no unnecessary personal data are included in the central repository and that access to any personal data or security-sensitive information is granted only on a need-to-know basis. The EDPS also recommends clarifying that the central repository should be designed, maintained and operated as a secure repository.

46. More generally, the EDPS recommends that the Proposal expressly provides that documentation already produced under EU data protection law — including records of processing activities, the agreements required under Article 28 GDPR and Article 29 EUDPR, transfer mapping and documented assessments of third-country law and practice — should be submitted as audit evidence under Annex III, in line with the approach reflected in recital 63, and, conversely, that audit evidence collected under the Proposal may be relied upon by controllers and processors as factual support for their accountability obligations, including their assessments of transfers of personal data. While factual evidence may be common to different legal frameworks, the legal conclusions drawn from them should remain specific to each framework.

[10] Annex III(2)(3)(b))

4.6. Article 29 risk assessments

47. Article 29 of the Proposal requires Member States and Union entities to carry out risk assessments in order to identify public sector activities that use or will make use of cloud computing services and that contribute to the preservation of public order. Those assessments are also intended to determine whether Union assurance level 2, 3 or 4 is appropriate for the identified public sector activities. Since Article 29 refers to obligations of Member States, the EDPS recommends clarifying which national authority or authorities should be responsible for carrying out, coordinating or validating those risk assessments at Member State level. The EDPS also recommends clarifying which Union entities are concerned by Article 29(1).

48. The EDPS understands that the risk assessment under Article 29 pursues objectives specific to the Proposal, namely the identification of the appropriate Union assurance level for public sector activities from the perspective of public order, sovereignty, operational autonomy, third-country access risks and service continuity.

49. The EDPS notes that Article 29(2)(a) refers, among other elements, to the "nature, scope, context and purpose of processing of personal data" and to the "risk of varying likelihood and severity for the rights and freedoms of data subjects". The EDPS recommends that the methodology, templates and elements to be specified by the Commission under Article 29(3) further clarify what is meant by those elements for the specific purposes of the Article 29 risk assessment, and how they should be weighed when determining the appropriate Union assurance level.

50. The EDPS further notes that Article 29(2)(a) uses terminology that mirrors concepts used in EU data protection law, in particular the reference to the nature, scope, context and purpose of the processing of personal data and to risks of varying likelihood and severity for the rights and freedoms of data subjects. Precisely for that reason, the EDPS considers that the methodology, templates and elements to be specified under Article 29(3) should ensure that those concepts are interpreted consistently with the GDPR and the EUDPR, while explaining how they are to be taken into account for the specific purpose of determining the appropriate Union assurance level under the Proposal. Against this background, the EDPS recommends that the methodology, templates and elements to be specified under Article 29(3) clarify how existing analyses, findings or documentation produced under EU data protection law may, where relevant, be taken into account for the purposes of the Article 29 assessment.

51. Given the direct bearing of the methodology, templates and elements to be specified under Article 29(3) on the processing of personal data by Union entities, the EDPS recommends ensuring that it be consulted on the implementing acts envisaged under that provision, in accordance with Article 42(1) EUDPR. Since the methodology is expected to provide a common framework for risk assessments carried out both by Union entities and by Member States, the EDPS also recommends that the Commission additionally consult the EDPB in accordance with Article 42(2) EUDPR.

52. In the spirit of simplification, the EDPS recommends that the methodology and templates to be adopted under Article 29(3) be designed so as to avoid duplication with existing assessment and accountability work carried out under EU data protection law. In particular, the methodology and templates to be adopted under Article 29(3) be designed as an integrated assessment framework, allowing Member States' authorities and Union entities to carry out the risk assessment under Article 29 and, where required, the data protection impact

assessment under Article 35 GDPR or Article 39 EUDPR as distinct chapters of a single exercise, based on a common description of the processing environment, the categories of data, the data flows and the relevant third-country exposure. The Commission should provide a mapping table identifying which elements serve both assessments. Such integration would reduce the administrative burden on public administrations without altering the distinct legal tests applicable under each framework.

53. The EDPS also notes that Article 29(1)(a) requires Member States and Union entities to identify public sector activities that "use or will make use" of cloud computing services. The identification of future cloud use may be difficult in practice, in particular where procurement needs, technical architecture or service models are not yet fully defined. The EDPS recommends that the methodology under Article 29(3) provide sufficient guidance on how future use should be identified and reviewed, while ensuring that the assessment remains concrete, proportionate and capable of being updated where the envisaged cloud use changes.

4.7. Public procurement, EuroCloud Federation and Commission-led procurement

54. The EDPS notes that the Proposal relies on public-sector demand as an important tool to promote the uptake of cloud computing services recognised under Union assurance levels. In particular, the Proposal lays down public procurement obligations, establishes the EuroCloud Federation and provides for Commission-led procurement and a common procurement framework.

55. The EDPS recommends that the procurement obligations under Article 30, the sharing conditions within the EuroCloud Federation under Article 35 and the Commission-led procurement framework under Articles 37 to 40 expressly ensure that, where cloud computing services are used for the processing of personal data, the relevant procurement and contractual arrangements enable contracting authorities, Union entities and public-sector bodies to comply with their obligations under EU data protection law. In particular, those arrangements should address, as appropriate, the allocation of controller and processor roles, processing instructions, sub-processing, access management, security of processing, international transfers and third-country access, logging and audit rights, incident management, business continuity and deletion or return of personal data.

56. The EDPS further notes that, pursuant to Article 30(3) of the Proposal, the cloud computing services procured by Union entities and public sector bodies in the areas of national security, internal security, external border management, defence, justice or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, must have a Union assurance level 2, 3 or 4. However, according to paragraph 4 of the same Article, in certain cases, contracting authorities may derogate from those requirements, including where applying the requirements of the Regulation would require the contracting authority to procure services at disproportionate cost.

57. The EDPS reminds that personal data processed for internal security, border management, justice, including criminal justice or law enforcement purposes are typically highly sensitive. In this context, a potential personal data breach, including access to the data by third countries or other unauthorised third parties, may have very serious consequences not only for the affected data subjects, but also for the competent Union or Member State authorities. The security of cloud services is also critical for Union agencies and large-scale IT systems in the

area of justice and home affairs, which act as information hubs and/or databases at Union level and may contain millions of records, including biometric data[11].

58. In the light of these concerns, the EDPS considers that the cloud computing services in the areas of internal security, border management, justice or law enforcement, procured by Union bodies, including eu-LISA, Europol, etc., must as a general rule have a Union assurance level 3 or 4, and recommends to the Union legislator to amend accordingly the Proposal.

59. The EDPS also considers that the possibility for contracting authorities to derogate from the applicable assurance-level requirements on grounds of disproportionate cost under Article 30(4) should be excluded, or strictly conditioned and duly documented, for the activities referred to in Article 30(3).

60. The EDPS also notes that assurance levels 2, 3 and 4 require access to source code for software components that are provided, owned and licensed by a legal entity established in a third country.[12] However, outside of open-source, access to source code is often difficult or even impossible to achieve (inter alia, software companies protect their intellectual property, patents and trade secrets...). This could lead to situations where no suitable candidates can meet this requirement and thus, achieve assurance levels 2, 3 or 4 and risks making Article 30(4) derogations the general rule.

61. The EDPS recommends clarifying the mechanisms under which a contracting authority can duly justify falling under the derogation in Article 30(4). This should include explaining under which point of Article 30(4) the derogation comes into play, specifying what steps were taken to meet the requirement of the derogation, and providing concrete evidence of the claimed statements. The EDPS also recommends that, where a derogation is used, proper risk management be performed, taking into account the specific context, including the cloud computing environment and the lack of access to source code. Risks should be analysed, compensating mitigating measures should be defined and the residual risks should be accepted.[13]

62. The EDPS further recommends requiring contracting authorities relying on Article 30(4) to regularly review the market and the central repository to verify whether new cloud computing services fully meet the required assurance level. Where such services become available, the contracting authority should migrate to a cloud computing service at the required assurance level within a strict timeframe. To ensure that generalised application of Article 30(4) does not go unnoticed, the EDPS also recommends requiring public authorities applying Article 30(4) derogations to notify the competent authority of the specific derogation point used and to provide the relevant justification.

63. As regards the sharing of data centre services and cloud computing services within the EuroCloud Federation, the EDPS recommends that the sharing conditions under Article 35

[11] See for instance Article 50 'Europol cloud infrastructure' of Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Union Agency for Law Enforcement Cooperation (Europol), amending Regulation (EU) 2018/1726 and Regulation (EU) 2024/982, and repealing Regulation (EU) 2016/794, COM(2026) 580 final.
[12] E.g. Annex II, 2. Union assurance level 2, 2.1 (i)(ii)
[13] Risks and mitigating measures are context specific but typical measures include, inter alia, encryption before uploading to the Cloud, clear documentation on the use and reuse of personal data, strict contractual clauses on the processing of personal data with substantial fines in case of non-compliance, regular security audits, logging and monitoring.

expressly require the allocation of the roles and responsibilities in accordance with Articles 26 or 28 GDPR or Article 28 or 29 EUDPR, as the case may be.

64. As regards the procurement activities of the Commission under Articles 37 to 40, the EDPS recommends, on the basis of lessons drawn from its supervisory practice concerning inter-institutional licence agreements, that the applicable framework contracts guarantee that each participating Union entity remains able to comply with its obligations as controller under the EUDPR, and that they secure, as non-negotiable terms, purpose limitation covering telemetry, metadata and service-generated data, full sub-processor transparency, complete transfer mapping, the handling of third-country authority requests in line with Article 49 EUDPR and Article 48 GDPR, audit rights exercisable by each controller and the unimpeded exercise of the powers of the EDPS under Article 58 EUDPR, including vis-à-vis processors. Where the Commission carries out procurement activities for the benefit of partner organisations which are neither Union entities nor contracting authorities of the Member States, the arrangements under Article 38 should identify the data protection framework applicable to their participation.

65. In the same vein, the EDPS recommends exploring the potential of the common procurement framework as a vehicle for integrated compliance. Model contractual clauses developed for the purposes of Articles 37 to 40 could be designed to satisfy simultaneously the requirements of Article 28 GDPR and Article 29 EUDPR and the relevant Union assurance criteria, where appropriate building on the standard contractual clauses adopted by the Commission for the relationship between controllers and processors and keeping in mind the procedural requirements for the development of such clauses under data protection law[14]. Likewise, the sharing conditions within the EuroCloud Federation could be standardised so as to serve at the same time as the arrangements required under Article 26 GDPR and Article 28 EUDPR in situations of joint controllership. A single, well-designed contractual architecture would deliver both sovereignty assurance and data protection compliance more reliably than parallel sets of instruments.

66. The EDPS notes that Article 35(6) empowers the Commission to adopt implementing acts specifying the procedure by which a sharing entity demonstrates that it fulfils the applicable technical, operational and organisational requirements[15]. The EDPS recommends that those implementing acts specify, at the appropriate level, the main steps of the assessment procedure, the information to be provided, the criteria to be applied and the possible review of the assessment. The EDPS further recommends that relevant information on the assessment of the sharing entity's technical, operational and organisational measures be made available, in a secure manner and subject to appropriate confidentiality safeguards, to the members of the EuroCloud Federation, so that they are duly informed of the level of security and resilience they may expect.

67. Where the Commission procures AI systems under Article 37, the EDPS recommends that the applicable procurement and contractual arrangements ensure that participating Union entities

[14] See Article 28(7) and (8) GDPR and Article 29(7) and (8) EUDPR. Standard contractual clauses for the matters referred to in Article 28(3) and (4) GDPR may be adopted either by the Commission, in accordance with the examination procedure referred to in Article 93(2) GDPR, or by a supervisory authority, in accordance with the consistency mechanism referred to in Article 63 GDPR. Under the EUDPR, standard contractual clauses for the matters referred to in Article 29(3) and (4) EUDPR may be adopted by the Commission or by the EDPS. See also Commission Implementing Decision (EU) 2021/915 on standard contractual clauses between controllers and processors under Article 28(7) GDPR and Article 29(7) EUDPR.

[15] Article 35(6) of the Proposal.

and contracting authorities receive sufficient information to assess and manage risks related to the processing of personal data, as well as relevant AI and cybersecurity risks. This may be particularly important where AI system providers limit the information made available on aspects such as training or validation data, system performance, limitations, security measures, data flows or possible bias. The procurement framework should therefore ensure that sufficient information is available to enable participating entities to comply with their respective obligations under EU data protection law and, where applicable, Regulation (EU) 2024/1689[16].

4.8. Competent authorities, cooperation and enforcement

68. Article 25 of the Proposal provides for the designation of national competent authorities responsible for the application and enforcement of the Union cloud sovereignty framework. It also establishes mechanisms for mutual assistance and cross-border cooperation between competent authorities and the Commission.

69. The EDPS welcomes that the recitals of the Proposal refer to cooperation with other relevant national authorities, including data protection authorities and cybersecurity authorities. However, the EDPS considers that, where the application of the Proposal concerns the protection of personal data, the role of data protection supervisory authorities should be more clearly reflected in the operative provisions.

70. This is particularly relevant where competent authorities under the Proposal assess, recognise, amend, suspend or revoke a Union assurance level, or where they rely on audits, audit evidence, repository information, transparency notifications or risk assessments that may concern the processing of personal data. In such cases, the Proposal should ensure that data protection supervisory authorities, the EDPB and the EDPS are associated where relevant, without prejudice to their respective tasks and powers under EU data protection law.

71. The EDPS recommends that the Proposal provide for an appropriate cooperation mechanism between the competent authorities designated under the Proposal, data protection supervisory authorities, the EDPS and, where relevant, cybersecurity authorities and authorities involved in the AI Act governance framework. Such mechanism should facilitate the exchange of relevant information and expertise in assessment, review and enforcement exercises, while preserving the distinct mandates and competences of each authority.

72. To the same end, the EDPS recommends that the cooperation mechanism enable coordinated or joint inquiries by competent authorities and data protection supervisory authorities concerning the same cloud computing service provider, allow the mutual use, as evidence in their respective procedures, of findings lawfully collected by the other authority, and give effect to the 'once-only' principle, so that providers are not subject to duplicate requests for the same information from different authorities.

73. The EDPS also draws attention to the risk of parallel sanctioning of the same conduct. An infringement such as enabling access by a third country or a third-country legal entity to

[16] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024.

customer data, or transferring customer data outside the Union contrary to the applicable assurance criteria, may simultaneously constitute an infringement of the Proposal, subject to penalties under Article 24, and an infringement of the GDPR or of the EUDPR, subject to the corrective powers and administrative fines of data protection supervisory authorities or of the EDPS. In light of Article 50 of the Charter of Fundamental Rights[17] and the case law of the Court of Justice on the duplication of proceedings and penalties[18], the EDPS recommends that the Proposal provide for mandatory coordination between the competent authorities and the data protection supervisory authorities concerned where proceedings relating to the same facts are envisaged or ongoing, including mutual information and the taking into account of penalties already imposed.

74. National competent authorities and market surveillance authorities designated under Regulation (EU) 2024/1689 are not included among the authorities named in Recital (59), notwithstanding that the cloud computing infrastructure recognised under Article 17 of the Proposal frequently underpins the AI systems that fall within the scope of that Regulation. The EDPS notes that Article 74(10) of the AI Act already requires Member States to facilitate coordination between market surveillance authorities and "other relevant national authorities or bodies... in other Union law" relevant to high-risk AI systems. The EDPS therefore recommends that Recital (59) of the Proposal be expressly extended to national competent authorities and market surveillance authorities designated under Regulation (EU) 2024/1689, including, insofar as Union entities are concerned, the European Data Protection Supervisor in its capacity under Article 74(9) thereof.

5. Additional comments

5.1. AI-related provisions and AI Act coherence

75. The EDPS observes that the Centres for AI, given their role under Article 5(3) in connecting organisations with the wider AI innovation ecosystem, could serve as a channel of access to testing and experimentation facilities' real-world testing capabilities in support of AI regulatory sandboxes under Articles 57 and 58 of Regulation (EU) 2024/1689. Whether this channel could extend further to support compliance-related actions under the AI Act for prospective providers and deployers of high-risk AI systems, as well as market surveillance authorities, is not addressed by the Proposal.

76. The EDPS therefore recommends that the Proposal clarify whether, and under what conditions, the Centres for AI, testing and experimentation facilities, AI factories and AI gigafactories may be used to support compliance and supervisory activities under Regulation (EU) 2024/1689, including compliance-related activities by providers and deployers of high-risk AI systems, the exercise by market surveillance authorities of their functions under Article 74 thereof, and the

[17] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391.
[18] See, in particular, Judgment of the Court of Justice of 22 March 2022, bpost SA v Autorité belge de la concurrence, C-117/20, EU:C:2022:202.

functioning of AI regulatory sandboxes under Articles 57 and 58 thereof, in addition to their role in supporting AI adoption.

77. The EDPS notes, in this connection, that Article 9(3) of the Proposal provides that the Union and the Member States shall endeavour to provide sufficient computing resources for, among other things, "public sector AI projects", without specifying whether this term is intended to include Union entities. This is distinct from the defined term "public sector body" in Article 2(6) of the Proposal, which, by reference to Article 2(1) of Directive (EU) 2019/1024[19], does not extend to Union entities as separately defined in Article 2(7). The EDPS considers that this ambiguity should be resolved, given the potential relevance of the infrastructure referred to in Article 9 for Union entities' capacity to meet their obligations under Regulation (EU) 2024/1689. The EDPS recommends that the Proposal clarify whether, and under what conditions, Union entities may access the infrastructure and services referred to in Article 9 of the Proposal, including by resolving the ambiguity regarding the scope of "public sector AI projects" under Article 9(3).

78. The EDPS also notes the references in the Proposal to the "AI first" principle, including in Article 5(2)(b). The EDPS also notes that the Apply AI Strategy, to which Recital (32) refers as the source of the definition of the "AI first" principle, does not provide an operational definition of that principle. Instead, it describes it as a shift in problem-solving posture whereby public sector organisations and private entities are encouraged to integrate AI into their business processes while weighing potential benefits and risks. Since this description lacks defined criteria, the EDPS considers that the "AI first" principle should be further clarified to strengthen legal certainty and consistency with other Union acts.

79. In light of the potential relevance of this principle for the deployment and uptake of AI systems, the EDPS recommends clarifying its meaning and ensuring that its implementation remains fully consistent with EU data protection law. In particular, the "AI first" principle should not be understood as affecting the application of the principles of necessity, proportionality, lawfulness, fairness, transparency, data minimisation, data protection by design and by default, security of processing and accountability.

80. The EDPS further considers that the risk-related language associated with the "AI first" principle is formulated in vague terms that are difficult to reconcile with the risk-based logic of Regulation (EU) 2024/1689. Recital (32) merely states that organisations should "take into consideration the potential risks" of AI adoption, without cross-referencing to the risk-based approach established under the AI Act. As a result, the Proposal promotes AI adoption while attaching a risk qualifier that lacks legal weight, where the AI Act establishes a tiered, obligation-bearing risk framework for the same subject matter. The EDPS recommends that the "AI first" principle be clarified so as to be applied in a manner consistent with the risk-based approach under the AI Act.

81. In relation to national cloud and AI strategies, the EDPS notes that Article 7(2)(h) refers to the accessibility of high-quality data for AI development. The EDPS recalls that measures intended to improve access to high-quality data for AI development must comply with EU data protection law where personal data are involved. This includes, where applicable, requirements

[19] 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 (recast), OJ L 172, 26.6.2019, p. 56.

relating to lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, security, accountability and data protection by design and by default.

82. The EDPS further notes that Article 7(2) of the Proposal, which sets out the mandatory content of national strategies, does not require Member States to address how their strategies for cloud and AI adoption relate to the compliance and oversight architecture already established under Regulation (EU) 2024/1689. Article 7(2), points (a) to (c), direct national strategies toward accelerating and broadening the adoption of AI across national, regional and local levels, and across strategic industrial and public sectors.

83. The EDPS notes that an increase in the pace and scale of AI adoption pursued under those points has a direct scaling effect on the population of AI systems in use and, consequently, on the volume of systems requiring risk classification, conformity assessment and market surveillance under Regulation (EU) 2024/1689. It may also increase the demand placed on national AI regulatory sandboxes and national competent authorities designated under that Regulation. The absence of any corresponding requirement in Article 7(2) to plan for the compliance and oversight consequences of the adoption it seeks to accelerate risks decoupling adoption planning from compliance planning at Member State level.

84. The EDPS therefore recommends that Article 7(2) be amended to require national strategies to also include measures for aligning national cloud and AI adoption planning with key compliance mechanisms under Regulation (EU) 2024/1689, including national AI regulatory sandboxes under Articles 57 and 58 thereof, conformity assessment procedures under Article 43 thereof, oversight of high-risk AI systems under Title III and Article 74 thereof, and cooperation with national competent authorities designated under that Regulation.

85. The EDPS notes that the coordination role assigned to the AI Board under Article 7(6) operates alongside other coordination and advisory functions referred to in the Proposal regarding Member States' cloud and AI adoption activities, including the Alliance for Industrial Data, Edge and Cloud and the Apply AI Alliance referred to in Recital (30), as well as the network of Centres for AI referred to in Article 5(6). Given the synergies and coverage of similar topics among these bodies, the EDPS suggests clarifying the specific role of the AI Board under Article 7(6) relative to the Alliance for Industrial Data, Edge and Cloud, the Apply AI Alliance and the network of Centres for AI, with a view to avoiding an unclear or overlapping division of coordination functions in respect of Member States' cloud and AI strategies.

86. The EDPS recommends that the Proposal better define the roles and relationships between the AI Board, the Alliance for Industrial Data, Edge and Cloud, the Apply AI Alliance and the Centres for AI. This clarification should specify, at the appropriate level, their respective focus areas, such as regulatory alignment with Regulation (EU) 2024/1689, industry engagement and local implementation.

5.2. Data centre acceleration zones, open-source solutions and technical elements

87. The EDPS notes Article 10(1) of the Proposal concerning data centre acceleration zones. To the extent that such provisions may have implications for the security, resilience or organisation of cloud infrastructure used for the processing of personal data, the EDPS recommends ensuring that appropriate technical and organisational safeguards are taken into account.

88. The EDPS welcomes Article 41 of the Proposal, which relates to using and facilitating the reuse of open standards and components released under an open-source licence when building cloud and AI ecosystems or stacks. Open-source solutions may contribute positively to the protection of personal data, in particular by enhancing transparency and auditability, since source code can be inspected and vulnerabilities, hidden functionalities or malicious functionalities may be more easily identified. Open-source solutions may also help reduce vendor lock-in.

89. At the same time, the EDPS notes that open-source solutions may also entail specific risks, including inconsistent maintenance, supply-chain vulnerabilities and the fact that visibility of source code may be used both by defenders and by attackers. The EDPS therefore recommends that the promotion of open-source solutions under the Proposal be accompanied, where appropriate, by adequate governance, security and maintenance safeguards. Properly implemented, open-source solutions can support compliance with data protection principles, in particular transparency, data minimisation, purpose limitation and security of processing.

90. The EDPS further notes that the terms "on-device edge" and "edge computing" are used in the Proposal but are not defined in Article 2. These concepts are important for understanding where potential processing of personal data takes place in relation to cloud services and AI systems. The EDPS therefore recommends clarifying those definitions.

6. Conclusions

91. In light of the above, the EDPS makes the following main recommendations:

(1) to insert a specific recital recalling the applicability of the GDPR, the EUDPR and, where applicable, the LED to any processing of personal data carried out in the context of the Proposal;

(2) to design the Union assurance framework as a complementary mechanism which may rely, where appropriate, on existing assessments, safeguards, evidence and audit results under EU data protection law, while preserving the distinct obligations of controllers and processors and the respective competences of data protection supervisory authorities and the EDPS;

(3) to clarify that recognition under a Union assurance level, conformity self-assessments, EU statements of conformity, audit reports, positive audit opinions and audit evidence under the Proposal do not amount to a recognition, certification, approval or finding of compliance with the GDPR or the EUDPR;

(4) to ensure that the relationship between the Union assurance criteria and audit evidence requirements in Annex II and Annex III and the requirements of EU data protection law is clearly articulated, in particular as regards subcontracting, outsourcing, data location, access to data, security measures, third-country access risks, audit evidence and technical documentation, and to avoid introducing notions that are close to, but not aligned with, the GDPR and the EUDPR;

(5) to address the technical inconsistencies identified in Annex II, in particular the cross-reference to Article 19 instead of Article 18, the apparent inconsistency between the data localisation criteria for Union assurance levels 2, 3 and 4, and the relationship between the requirement that certain data are not transferred outside the Union "in any case" and the possibility for the public sector body to "explicitly require otherwise";

(6) to clarify the interaction between the data localisation requirements in Annex II and Chapter V of the GDPR and of the EUDPR, in particular by anchoring the personal data dimension of those requirements, where appropriate, in Article 49(5) GDPR and Article 50(5) EUDPR. At a minimum, the Proposal should clarify that nothing in the Proposal authorises or exempts transfers of personal data from the requirements of Chapter V of the GDPR or of the EUDPR, and that customer-approved carve-outs in Annex II do not constitute self-standing authorisations for transfers of personal data;

(7) to clarify the relationship between Article 18 of the Proposal and adequacy decisions under Article 45 GDPR, including the consequences of the suspension, repeal, amendment or invalidation of the adequacy decision underlying an implementing act adopted pursuant to Article 18, as well as appropriate transition arrangements for cloud computing services already procured at Union assurance level 3;

(8) to clarify whether, and under what conditions, a cloud computing service provider established in the Union but controlled by a parent company established in a third country is to be considered subject to the control of a third country or of a legal entity established in a third country for the purposes of the Proposal;

(9) to ensure that audits, audit evidence and the central repository are subject to appropriate safeguards, including purpose limitation, confidentiality, security, retention limits and data minimisation. In particular, the EDPS recommends limiting the collection of personnel data for the verification of Union citizenship to what is strictly necessary, favouring documented attestations over the collection and retention of identity documents, and reframing Annex III so that auditing organisations verify factual elements without assessing or certifying conformity with the GDPR or the EUDPR;

(10) to clarify the methodology, templates and elements to be specified under Article 29(3), including the meaning and weighting of the criteria referred to in Article 29(2)(a), as well as the national authorities responsible for carrying out, coordinating or validating the assessments, and the Union entities concerned. The methodology should allow existing factual analyses and documentation produced under EU data protection law to be taken into account where relevant, without treating the Article 29 assessment as equivalent to, or replacing, any assessment required under the GDPR or the EUDPR;

(11) to ensure consultation of the EDPS and EDPB on the implementing acts envisaged under Article 29(3) in accordance with Article 42(2) EUDPR;

(12) to strengthen the data protection safeguards applicable to public procurement, the EuroCloud Federation and Commission-led procurement. In particular, the Proposal should ensure that the relevant procurement and contractual arrangements clearly allocate the applicable data protection roles and responsibilities, include the necessary instruments under the GDPR and the EUDPR, and enable Union entities, public sector bodies and contracting authorities to comply with their obligations under EU data protection law;

(13) to require, as a general rule, Union assurance level 3 or 4 for cloud computing services procured by Union bodies in the areas of internal security, border management, justice and law enforcement, and to exclude or strictly condition and duly document the cost-based derogation under Article 30(4) for those activities;

(14) to ensure that framework contracts concluded under Articles 37 to 40 contain appropriate and non-negotiable data protection safeguards, including purpose limitation for telemetry, metadata and service-generated data, full sub-processor transparency, complete transfer mapping, appropriate handling of third-country authority requests, audit rights for each controller and the unimpeded exercise of the EDPS' powers under Article 58 EUDPR;

(15) to establish an appropriate cooperation mechanism between the competent authorities designated under the Proposal, data protection supervisory authorities, the EDPS and, where relevant, cybersecurity authorities and authorities involved in the AI Act governance framework. Such mechanism should facilitate the exchange of relevant information and expertise, enable coordinated or joint inquiries where appropriate, avoid duplicate requests for the same information and ensure coordination where proceedings relating to the same facts are envisaged or ongoing;

(16) to ensure that national cloud and AI strategies are aligned with key compliance mechanisms under Regulation (EU) 2024/1689, including national AI regulatory sandboxes, conformity assessment procedures, oversight of high-risk AI systems and cooperation with national competent authorities designated under that Regulation, and to clarify the "AI first" principle in order to strengthen legal certainty and consistency with EU data protection law and other Union acts;

(17) to clarify the roles and relationships between the AI Board, the Alliance for Industrial Data, Edge and Cloud, the Apply AI Alliance and the Centres for AI, in particular as regards their respective focus areas, including regulatory alignment with Regulation (EU) 2024/1689, industry engagement and local implementation;

(18) to ensure that the provisions on data centre acceleration zones, open-source solutions and technical elements are accompanied, where relevant, by appropriate technical, organisational, governance, security and maintenance safeguards, and to clarify the definitions of "on-device edge" and "edge computing".

Brussels,

Wojciech Wiewiórowski

Digitally signed by:
WOJCIECH RAFAŁ
WIEWIÓROWSKI (EUROPEAN
DATA PROTECTION SUPERVISOR)
Date: 2026-07-29 12:18:31 UTC