Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2025/0360 (COD)

Brussels, 20 February 2026

WK 2859/2026 INIT

LIMITE

SIMPL
ANTICI
DATAPROTECT
CYBER
TELECOM
CODEC
PROCIV
COMPET
MI

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

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Antici Group (Simplification)
Subject:	Omnibus VII (Digital Omnibus) – EDPB-EDPS Joint opinion on the Digital Omnibus

In view of the upcoming meeting of the Antici Group (Simplification) of 27 February 2026 relating to Omnibus VII (Digital Omnibus), delegations will find attached the EDPB-EDPS Joint opinion on the Digital Omnibus.

EDPB European Data Protection Board

EDPS

PUBLIC

EDPB-EDPS JOINT OPINION 2/2026

On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus)

Adopted on 10 February 2026



Table of Contents

1 Background 7

I. Changes relating to the GDPR and the ePrivacy Directive 8

2 General remarks 8

3 Definition of personal data 9

3.1 Changes to the definition of personal data 9

3.2 Implementing acts to clarify whether data resulting from pseudonymisation constitutes personal data for certain entities 11

4 Scientific research 12

4.1 Definition 12

4.2 Purpose limitation 14

4.3 Transparency 14

4.4 Recital on scientific research and legitimate interest 15

5 Exemption to allow the processing of biometric data 15

6 Artificial intelligence: legitimate interest and exemption to process special categories of personal data 16

6.1 Use of legitimate interest in the context of AI models/systems 16

6.2 Additional exemption for incidental and residual processing of special categories of data in the context of the development and operation of an AI system or model 18

7 Rights of data subjects 19

7.1 Limitation to data subject access requests 19

7.2 Transparency: Exemption to the provision of information where personal data are collected from the data subject 21

7.3 Automated individual decision-making 22

8 Data breaches 23

8.1 Notifications 23

8.2 Common EDPB template and list of circumstances 25

8.3 Single-entry point (SEP) 26

9 Data Protection Impact Assessment 26

9.1 Common EDPB DPIA lists 26

9.2 Common EDPB template and methodology for DPIA 27

10 ePrivacy provisions: Protection of terminal equipment and security of processing 28

10.1 Changes to the protection of information stored or accessed in terminal equipment 28

10.2 Automated and machine-readable indications of data subject's choices 32

10.3 Repeal of Article 4 ePrivacy Directive 34

II. Changes relating to the Data Acquis 34

11 General remarks 34

PUBLIC

12 Making data available in case of a public emergency....35
12.1 Circumstances when personal and non-personal data can be requested....35
12.2 Definition and implementation of technical and organisational measures....36
12.3 Notification of the request for data by the public sector body to the DPA....36
13 Changes to the data intermediation services and altruism organisations....37
13.1 Changes specific to data intermediation services....37
13.1.1 Voluntary registration of data intermediation services instead of mandatory prior notification....37
13.1.2 Functional instead of legal separation of data intermediation services from other services....39
13.2 Changes specific to data altruism organisations....39
13.3 Application forms for registering data intermediation service providers and data altruism organisations....40
13.4 Competent authorities for the registration of data intermediation services providers and data altruism organisations....41
14 Re-use of data and documents held by public sector bodies....41
15 Enforcement by and cooperation between competent authorities and other authorities 43
15.1 Horizontal application of the implementation and enforcement provisions of the proposed Data Act....43
15.1.1 Designation of competent authorities to oversee Proposed Chapter V Data Act and relationship with horizontal oversight provisions in Proposed Chapter IX Data Act 43
15.1.2 Right to lodge a complaint regarding Proposed Chapter V and relationship with horizontal complaint provisions in Chapter IX Proposed Data Act....44
15.1.3 Specific redress mechanism for the re-use of public sector data in Proposed Chapter VIIc and relationship with horizontal redress provisions in Proposed Chapter IX Data Act 44
15.2 Cooperation and information exchange between competent authorities and other relevant authorities....44
15.3 Clarification of Articles 37(3) and 40(4) Data Act....45
16 EDIB: changes to structure and role....46

PUBLIC

Executive summary

On 19 November 2025, the European Commission (the 'Commission') issued a Digital Omnibus proposal[1] amending a large corpus of the EU digital legislation, including the GDPR, the Single Digital Gateway Regulation, the EUDPR, the Data Act, the ePrivacy Directive, the Cybersecurity Directive, NIS 2, and the Data Governance Act ('the Proposal').

The EDPB and the EDPS support the Proposal's aim to simplify compliance with the digital rulebook, strengthen the effective exercise of individual rights, and boost EU competitiveness. These goals echo the Helsinki Statement, where the EDPB committed to take up initiatives facilitating GDPR compliance and strengthening consistency[2]. The EDPB and the EDPS underline the importance that the proposed simplifications clarify obligations and bring legal certainty while maintaining trust and a high level of protection of individual rights and freedoms.

Changes relating to the GDPR/EUDPR

The EDPB and the EDPS welcome the parts of the Proposal that may foster greater harmonisation, consistency and legal certainty, or reduce unnecessary administrative burden. In this regard, they **welcome the proposed changes on the following topics**, and suggest certain improvements:

- **scientific research**, in particular the introduction of a definition; the clarification that Article 6(4) GDPR does not need to be applied; as well as the new (limited) derogation to the duty to inform.
- the **new exception for the processing of special categories of data for biometric authentication**, where the verification means are under the individual's sole control.
- **data breach notifications and data protection impact assessments** ('DPIAs'), in particular increasing the notification threshold and extending the deadline, as well as establishing data breach notification and DPIA common templates and lists. However, the EDPB should be fully entrusted with both the preparation *and* approval of such documents, and the EDPS should be entrusted with corresponding competences under the EUDPR.

At the same time, the EDPB and the EDPS consider that **the following proposed changes raise significant concerns** as they will adversely affect the level of protection enjoyed by individuals, create legal uncertainties and/or make it more difficult to apply the law in practice:

- the proposed changes to the **definition of personal data** would narrow the concept of personal data and would adversely affect the fundamental right to data protection. The proposed changes go far beyond a targeted modification of the GDPR, a 'technical amendment' or a mere codification of CJEU jurisprudence. For these reasons the EDPB and the EDPS strongly urge the co-legislators to not adopt the proposed changes to the definition of personal data.
- Defining what is no longer personal data after pseudonymisation also directly affects the scope of application of EU data protection law and should not be addressed in an **implementing act**.

[1] Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/1679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus).
[2] EDPB's Helsinki Statement on enhanced clarity, support and engagement, A fundamental rights approach to innovation and competitiveness, adopted on 2 July 2025.

Furthermore, the EDPB and the EDPS **support the Proposal's underlying aim for the proposed changes on the following topics, though they believe that improvements are necessary**:

- **use of legitimate interest in the context of AI**: As the EDPB has already explicitly confirmed this in its Opinion 28/2024 on AI models, it does not appear necessary to insert a specific provision to this effect. The Joint Opinion nevertheless provides specific suggestions, including on the legitimate interest assessment and on the right to object, should the co-legislators wish to proceed with this change.
- **an exception for incidental and residual processing of special categories of data in the context of AI:** The EDPB and the EDPS acknowledge that when data is collected for the training, testing and validation of certain AI systems or models, it is not always possible to avoid residual and incidental processing of special categories of data. The Joint Opinion recommends several improvements, such as referring to 'incidental and residual' in the enacting terms, clarifying the scope of the derogation, and ensuring safeguards throughout the whole lifecycle.
- **limitation to the right of access**: Clarifying what qualifies as an abuse of rights is welcome, but it should not be linked to the exercise of the right to access for purposes other than data protection, as the GDPR also aims to protect other fundamental rights and freedoms. The Joint Opinion makes specific suggestions, such as linking 'abuse of rights' to the existence of an abusive intention. In addition, the EDPB and the EDPS underline that Article 12(5) GDPR is currently mirrored in Article 57(4) GDPR and that this should be maintained. Therefore, supervisory authorities should continue to be able to refuse to act on a complaint or to charge a reasonable fee under the same conditions as a controller would be able to refuse to grant a request for access, provided that the remarks regarding Article 12(5) GDPR are duly taken into account.
- **new derogation for transparency**: Simplifying information requirements and reducing administrative burden, in particular for SMEs, is welcome, but the Joint Opinion suggests clarifications to ensure legal certainty, effectively reduce the burden, and ensure that individuals may still receive information about their data.
- **automated individual decision-making:** The prohibition in principle, as it was clarified by the CJEU, should be retained. The Joint Opinion provides a concrete suggestion to retain this principle with exceptions. The EDPB and the EDPS welcome the aim of clarifying the exceptions to the current prohibition but suggest amendments to avoid implying that automated decision-making is in principle allowed whenever there is a contract regardless of whether it is 'necessary'. They also provide suggestions to further clarify what assessing 'necessity' entails.

Finally, the EDPB and the EDPS welcome the intention to ensure alignment of the EUDPR and GDPR. They underline the need to ensure legal certainty and uniform application of equivalent data protection standards across the Union by private and public organisations, including EU institutions, agencies and bodies. At the same time, this Joint Opinion also identifies specific cases where full alignment between texts does not seem appropriate, and adaptations are needed.

Changes relating to the ePrivacy Directive

The EDPB and the EDPS strongly support the aim of the Proposal to provide for a regulatory solution to address consent fatigue and proliferation of cookie banners and to simplify the rules applicable to the protection of the terminal equipment of end-users. The EDPB and the EDPS also generally welcome that the Proposal aims to provide limited additional derogations to the general prohibition to store or gain access to personal data in the terminal equipment (subject to specific recommendations) and the fact that the oversight of such matters will be entrusted

to the supervisory authorities established in accordance with the GDPR to further support regulatory consistency. That being said, the EDPB and the EDPS are concerned that the proposed separation of the rules on access to and storage of information in terminal equipment over different legal instruments may lead to legal uncertainty. The Joint Opinion also provides additional recommendations to enhance legal certainty, minimise the risks and foster responsible innovation, including by adding an exception for contextual advertising.

The Joint Opinion highlights that entrusting data protection authorities with the oversight of these new rules cannot be implemented without ensuring effective corrective powers.

Changes relating to the Data Acquis

In the second part of the Joint Opinion, the EDPB and the EDPS address key changes introduced by the Proposal in the data legislative acquis ('Data Acquis'). The EDPB and the EDPS welcome clarifications as well as streamlining of the rules. In particular, the EDPB and the EDPS welcome the integration of the Data Governance Act ('DGA') and Open Data Directive ('ODD') rules on the re-use of data and documents held by public sector bodies into the Data Act, which will simplify compliance and the application of the rules.

In relation to access granted by public bodies for re-use, the EDPB and the EDPS recommend maintaining the provisions which clarify that the legal framework does not in itself create any obligation on public sector bodies to allow re-use of personal data, and that it does not provide a legal basis for granting access.

Regarding the duties to make data available to public sector bodies in case of public emergencies, the EDPB and the EDPS recommend affirming that personal data – in pseudonymised form only – can be shared, where anonymous data is insufficient to respond to an exceptional need for data.

In the area of data intermediation services and data altruism organisations, the EDPB and the EDPS highlight the importance of trustworthy and responsible data sharing. They recommend maintaining specific safeguards, favouring transparency and oversight.

Regarding enforcement, the EDPB and the EDPS recommend including provisions to enable the exchange of information on enforcement activities among authorities competent under the Data Act and other regulatory authorities, such as supervisory authorities. They also recommend clarifying the responsibilities and competences of supervisory authorities in terms of monitoring and enforcing the Data Act.

The EDPB and the EDPS welcome the Proposal's confirmation of the EDIB's role in supporting the consistent application of the Data Act. They recommend clarifying that the EDIB will continue to assist the Commission in the development of guidelines and standards. They also recommend empowering the Commission to issue guidelines on any topic concerning the Data Act. This would enable the Commission to develop joint guidelines with the EDPB, and allow the EDIB to advise and assist the Commission in the development of such guidelines.

The European Data Protection Board and the European Data Protection Supervisor

Having regard to Article 42(2) of the Regulation 2018/1725 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.

Have adopted the following joint opinion

1 BACKGROUND

1. On 19 November 2025, the European Commission ('the Commission') issued a Digital Omnibus proposal[3] amending a large corpus of the EU digital legislation, including the GDPR, the Single Digital Gateway Regulation, the EUDPR, the Data Act, the ePrivacy Directive, the Cybersecurity Directive, NIS 2, and the Data Governance Act (hereinafter, 'the Proposal'). On 25 November 2025, the Commission formally consulted the EDPB and the EDPS in accordance with Article 42(2) of Regulation (EU) 2018/1725 ('EUDPR')[4].
2. The Commission selected those acts as part of a broader stress-testing of the digital rulebook, to bring relief to businesses, public administrations, and citizens alike. According to the Commission, targeted amendments concerning the GDPR[5], the EUDPR, and the ePrivacy Directive[6] aim to implement feedback from stakeholders and address compliance challenges in order to foster opportunities for the use of data and to provide immediate simplification measures for businesses and individuals, strengthening their ability to exercise their rights[7]. They seek to provide clarity and predictability in the application of existing rules, and to reduce administrative burden, without undermining the high level of data protection under the GDPR and EUDPR[8]. The Proposal also aims to reflect proposed amendments to the GDPR in the EUDPR where relevant, in order to maintain a strong and coherent EU data protection framework and ensure a consistent interpretation.

[3] Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/1679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus).
[4] 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, pages 39–98.
[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), OJ L 119, 4.5.2016, pages 1–88.
[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, pp. 37–47.
[7] Proposal, COM(2025) 836 final, Explanatory Memorandum, p. 2.
[8] Proposal, COM(2025) 836 final, Explanatory Memorandum, p. 3. See also p. 33 of the Commission Staff Working Document (SWD(2025) 836 final) accompanying the Proposal ('Commission Staff Working Document').

3. Amendments concerning the Data Act[9], the Data Governance Act[10], the Free Flow of Non-Personal Data Regulation[11], and the Open Data Directive[12] ('the Data Acquis') propose to integrate relevant provisions from the Data Governance Act, the Free Flow of Non-Personal Data Regulation and the Open Data Directive into the Data Act, and to repeal the former acts. In doing so, the Commission seeks to bring the rules supporting a competitive single market for data sharing and use into one coherent law[13].

I. Changes relating to the GDPR and the ePrivacy Directive

2 GENERAL REMARKS

4. The EDPB and the EDPS welcome the Proposal's objectives to optimise the application of the digital rulebook, simplify compliance with the rules, strengthen individuals' ability to exercise their rights, and stimulate competitiveness[14]. These goals echo the EDPB's commitments in its Helsinki Statement to take up initiatives to facilitate GDPR compliance and strengthen consistency[15], in order to empower responsible innovation and reinforce competitiveness in Europe. The EDPB and the EDPS underline the importance of the Commission's commitment that the proposed amendments clarify obligations and bring legal certainty while maintaining trust and ensuring a high level of fundamental rights and freedoms of individuals[16].
5. The EDPB and the EDPS welcome the parts of the Proposal that have the potential of fostering greater harmonisation, consistency and legal certainty or reduce unnecessary administrative burden. In particular, they welcome the changes relating to processing for scientific research, the notification of data breaches, data protection impact assessments and the new exception enabling the processing of biometric data for authentication purposes where the verification means are under the sole control of the individual. Certain improvements are suggested, mainly with a view of enhancing clarity and legal certainty and preserving the independence and competence of the EDPB and the EDPS.
6. The EDPB and the EDPS express significant concerns regarding certain proposed changes to the definition of personal data and the possible use of implementing acts to define the effects of pseudonymisation. These changes will, contrary to the stated and intended goals of the Proposal, actually generate new legal uncertainties, make it more difficult to apply the law in practice, adversely affect the level of protection enjoyed by individuals and/or make it more difficult for data subjects to exercise their rights. Furthermore, the EDPB and the EDPS consider that certain changes proposed on the notion of personal data are not merely of a 'technical' nature and go beyond a 'targeted update'.

[9] 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), OJ L, 22.12.2023.
[10] 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 152/1, pp. 1–44.
[11] 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, pp. 59–68.
[12] 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, pp. 56–83.
[13] See p. 8 of the Commission Staff Working Document.
[14] Proposal, COM(2025) 836 final, Explanatory Memorandum, p. 2.
[15] EDPB's Helsinki Statement on enhanced clarity, support and engagement, A fundamental rights approach to innovation and competitiveness, adopted on 2 July 2025.
[16] Proposal, COM(2025) 836 final, Explanatory Memorandum, p. 3.

7. The EDPB and the EDPS regret that the Proposal was not accompanied by a full impact assessment and consider that insufficient consideration has been given to the adverse effects of certain proposed changes on the protection of fundamental rights and freedoms of individuals. In this regard, the EDPB and the EDPS recommend to pay specific attention to the impact of these amendments on the fundamental rights and freedoms of individuals in the next regular evaluations and reviews that will take place under Article 97 GDPR, if the amendments are adopted.
8. While the EDPB and the EDPS support the intention underlying certain other proposed changes, they consider that improvements are necessary as outlined in this Joint Opinion. This includes the use of legitimate interest in context of AI, the exception for incidental and residual processing of special categories of data in the context of AI, the limitation to the right of access and the new derogation for transparency, and the changes on automated decision-making.
9. In relation to the changes to the ePrivacy Directive, the EDPB and the EDPS strongly support simplifying the rules applicable to the protection of the terminal equipment of end-users. They also generally welcome that the Proposal aims to provide limited additional derogations to the general prohibition to store or gain access to personal data in the terminal equipment and the fact that the oversight of such matters will be entrusted to the supervisory authorities established in accordance with the GDPR. That being said, they are concerned that the proposed separation of the rules on access to and storage of information in terminal equipment over different legal instruments may lead to legal uncertainty.
10. Lastly, the EDPB and the EDPS welcome the intention to ensure alignment of the EUDPR and GDPR, and underline the need to ensure legal certainty and uniform application of equivalent data protection standards across the Union by private and public organisations, and by the EU institutions, agencies and bodies. Unless otherwise specified, the EDPB and the EDPS comments included in this Joint Opinion with regard to proposals for amendments to the GDPR also apply to the corresponding proposals for amendments to the EUDPR. At the same time, this Joint Opinion also identifies specific cases where full alignment between texts does not seem appropriate and adaptations are needed.

3 DEFINITION OF PERSONAL DATA

3.1 Changes to the definition of personal data

11. The Proposal would add a new paragraph under Article 4(1) GDPR and Article 3(1) EUDPR to the definition of personal data as follows: 'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates'[17].
12. The proposed amendments 'seek to codify interpretations of the Court of Justice of the European Union (CJEU), such as with regard to pseudonymisation of personal data'[18], in particular the judgment in case C-413/23 P (the 'EDPS v SRB judgment')[19].

[17] See Article 3(1) and 4(1) Proposal.
[18] Proposal, COM(2025) 836 final, Explanatory Memorandum, p. 10.
[19] Judgment of the Court of Justice of 4 September 2025, EDPS v SRB, C-413/23 P, ECLI:EU:C:2025:645.

13. However, as will be shown below, the proposed amendments introduce significant changes to this definition that go beyond the stated aim of introducing 'targeted' or 'technical' amendments to the GDPR and EUDPR.

14. The EDPB and the EDPS emphasise that the definition of personal data lies at the very core of EU data protection law, including Article 8 of the Charter of Fundamental Rights (the 'Charter') and Article 16 of the Treaty on the Functioning of the EU. Modifying the definition of personal data would directly impact the material scope of the GDPR and EUDPR.

15. The EDPB and the EDPS emphasise that the GDPR and EUDPR – including the definition of personal data – must in any case be interpreted in light of the whole body of CJEU jurisprudence. A selective codification of that case-law, as contained in the Proposal, introducing only a single element from a single case, lacks the necessary context[20]. The Proposal ignores the specific characteristics of the case and will undermine – rather than improve – legal certainty.

16. In addition, the EDPB and the EDPS highlight that the proposed changes do not accurately reflect and clearly go beyond the CJEU jurisprudence. This is the case, in particular, of the last sentence of the proposed new text which specifies that 'such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates'[21]. In the EDPS v SRB judgment, the CJEU confirmed its previous jurisprudence[22], by recalling that otherwise impersonal data may become personal in nature when they are put at the disposal of a recipient (any recipient) with means reasonably likely to be used to identify a data subject[23]. The CJEU confirmed that, in such cases, those data are personal data both for the recipient and, indirectly, for the entity making the data available to the latter[24].

17. In this respect, the EDPB and the EDPS consider that the proposed changes would result in significantly narrowing the concept of personal data, thereby adversely affecting the fundamental right to data protection. Moreover, the proposed change may induce controllers to seek loopholes in the data protection regime and try to circumvent the application of the GDPR or the EUDPR[25]. The Proposal further overlooks key elements of the concept of personal data under Recital 26 GDPR such as the concept of 'singling out'[26].

18. Furthermore, the EDPB and the EDPS consider that the proposed new text would create confusion and would not meet the much-desired need for legal clarity. In the view of the EDPB and the EDPS, the definition should say what personal data is, instead of what it is not. A 'negative' definition such as the one proposed by the Commission is likely to increase legal uncertainty. In addition, to ensure legal clarity, the definition should avoid using undefined legal terms[27].

---

[20] Selective codification of specific elements from one specific case may also lead to more legal uncertainty as regards other cases (or elements of those cases) which have not been codified.

[21] This provision is clarified in Recital 27 Proposal: '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'.

[22] Judgment of the Court of Justice of 9 November 2023, Gesamtverband Autoteile-Handel eV v Scania CV AB, C-319/22, ECLI:EU:C:2023:837, paragraphs 46 and 49.

[23] See EDPS v SRB judgment, paragraphs 84 and 85.

[24] See EDPS v SRB judgment, paragraphs 84 and 85.

[25] In particular, there is a risk that controllers could implement nominal measures to separate their processing activities from the means reasonably likely to be used to identify the data subjects, seeking to remove them from the scope of the GDPR/EUDPR, while still allowing for abuse of data subjects' personal data. This could include, for example, artificially outsourcing certain activities or capabilities to external companies, using a structure which deliberately avoids the limitations and protections that come from meaningful anonymisation techniques.

[26] This is particularly relevant in the context of online advertising.

[27] The EDPB and the EDPS note that the expression 'entity' used in the Proposal qualifies as an undefined legal term which is used in the GDPR only in its Article 47 in a different context.

19. In this respect, the EDPB and the EDPS recall that the EDPB is preparing updated guidance on pseudonymisation following a public consultation and developing a new set of guidelines on anonymisation, which will take into account, among others, the EDPS v SRB judgment[28]. This consultation demonstrated that this new ruling raises numerous practical and legal questions[29], also taking into consideration the rest of the body of CJEU case law. The EDPB and the EDPS consider that such questions are better addressed through further EDPB guidance, that supports organisations in their practice and takes into account all the body of jurisprudence, rather than by amending the definition itself. The EDPB guidance will also offer clarification on the implications of the EDPS v SRB judgment on other provisions of the GDPR, including Articles 26 and 28 GDPR and Chapter V GDPR.

20. In addition, the EDPB and the EDPS note that the definition of personal data contained in the GDPR is referred to by or aligned with other important EU legal acts, such as Directive (EU) 2016/680[30]. Changing the definition of personal data in the GDPR could thus have unintended repercussions on other legal acts and may undermine the overall coherence of the EU legal framework[31].

21. In short, the proposed amendment goes far beyond a targeted modification of the GDPR, a 'technical amendment' or a mere codification of CJEU jurisprudence. In addition, the proposed amendment would also result in a more restrictive interpretation of the concept of personal data, limit the scope of application of the GDPR, and thus negatively affect the protection of the fundamental rights and freedoms of individuals while increasing legal uncertainty for organisations. For these reasons, the EDPB and the EDPS strongly urge the co-legislators to not adopt the proposed changes to the definition of personal data.

3.2 Implementing acts to clarify whether data resulting from pseudonymisation constitutes personal data for certain entities

22. A newly proposed Article 41a GDPR would empower the Commission to adopt implementing acts to specify means and criteria to determine whether data resulting from pseudonymisation no longer constitute personal data for certain entities[32]. This amendment would complement the proposed change to the definition of personal data[33].

[28] In this context, in addition to the written consultation on the first version of the guidelines on pseudonymisation (EDPB Guidelines 01/2025 on Pseudonymisation, adopted on 16 January 2025, version for public consultation) which was organised before the EDPS v SRB judgment, the EDPB held a stakeholder event on 12 December 2025 on anonymisation and pseudonymisation, to collect input from individuals representing sector associations, organisations or NGOs and individual companies, law firms or academics following the EDPS v SRB judgment.

[29] For example, the questions asked by stakeholders include the following: if an entity receiving the data does not have the means reasonably likely to identify the data subject but processes those data on behalf of the data controller, can it be qualified as a data processor (i.e., an entity that processes personal data on behalf of the data controller)? Alternatively, if the recipient does not have the means to identify the data subject but participates in defining the purpose of the processing, could it be qualified as joint controller?

[30] 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, pp. 89–131.

[31] The EDPB and the EDPS also note that any changes affecting substantially the definition of personal data under the GDPR might also create risks of fragmentation with other international legal frameworks – such as in particular Convention 108 or Convention 108+ of the Council of Europe – or national laws in third countries that so far are largely aligned or equivalent to the current definition under the GDPR.

[32] The common criteria adopted by the Commission and referred to in proposed Article 41a GDPR would also apply to the processing of personal data under the EUDPR. See Article 4(9) Proposal.

[33] See Recital 27 Proposal.

23. The EDPB and the EDPS are concerned that the Proposal would allow for the further specification – by way of an implementing act – of the means and criteria that determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities. As explained above, the delineation of what constitutes (and what does not constitute) personal data directly affects the scope of application of EU data protection law. An implementing act as proposed could de facto affect the material scope of EU data protection law, effectively redefining the scope of when and for whom information is considered personal data. The EDPB and the EDPS consider that it should be the competence of supervisory authorities, under the control of the competent courts, to apply the definitions of the GDPR in an independent manner as guaranteed by Article 8(3) of the Charter and it is the competence of the EDPB to ensure consistent application on this matter[34].

24. Additionally, the EDPB and the EDPS have serious doubts whether the implementing acts would precisely facilitate compliance for controllers and offer increased legal certainty. On the one hand, the draft provision would empower the Commission to specify means and criteria to determine whether data resulting from pseudonymisation no longer constitute personal data for certain entities[35]. On the other hand, the provision indicates that the implementation of the means and criteria outlined in an implementing act 'may be used as an element' to demonstrate that data cannot lead to reidentification of the data subjects. The EDPB and the EDPS consider that the practical impact of implementing the 'means and criteria' set out in the implementing acts remains unclear and leads to difficulties for compliance (e.g. whether or not this would form a rebuttable presumption of non-identifiability or merely serve as one factor among others). This will likely result in more complexity and confusion for public and private entities, which would be contrary to the declared simplification objective of the Proposal.

25. For all the above reasons, the EDPB and the EDPS therefore suggest deleting proposed Article 41a GDPR from the Proposal.

4 SCIENTIFIC RESEARCH

4.1 Definition

26. The EDPB and the EDPS welcome the Proposal's aim of harmonising the notion of 'scientific research' in the context of the GDPR and EUDPR as this can enhance legal certainty and help to support scientific research. The proposed definition incorporates several key elements, in particular the conditions that scientific research '(...) shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing and adhere to ethical standards in the relevant research area'.

[34] For the EUDPR, the EDPS has the responsibility of monitoring and ensuring its application throughout the Union for Union Institutions, bodies and entities.

[35] Through an implementing act under Article 8(2) DMA, the Commission may specify legally binding measures on gatekeepers to ensure effective anonymisation and on the eligibility of third parties to receive data under Article 6(11) DMA. Such legally binding measures may prescribe conditions and safeguards under which a gatekeeper must share data with eligible third parties under Article 6(11) DMA. See Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation, paragraphs 188-189. The implementing acts adopted under Article 8(2) DMA are firmly different to the one proposed in Article 41a GDPR. While Article 8(2) DMA empowers the Commission as enforcer of the DMA to specify the measures that the gatekeeper concerned is to implement in order to effectively comply with the obligations laid down in the DMA, the proposed Article 41a GDPR allows the Commission to set out general means and criteria applicable to all controllers for assessing whether data resulting from pseudonymisation no longer constitutes personal data.

27. The EDPB and the EDPS welcome the aforementioned elements included in the proposed definition. In addition, the EDPB and the EDPS recommend that the co-legislators further delineate what constitutes scientific research in the context of the GDPR and EUDPR. This would help ensure that the proposed definition leads to the envisaged harmonisation between Member States, addresses the current fragmentation and meets the goal of simplification.

28. Having a clear, precise and well delineated definition is also important because the definition will affect the applicability of all other provisions in the GDPR and EUDPR that apply to processing of personal data for scientific research purposes, including Articles 5(1)(b) and (e), 14(5)(b), 17(3)(d), 21(6) and 89 GDPR and Articles 4(1)(b) and (e), 13, 16(5)(b), 19(3)(d), 23(4) and 25(3) EUDPR[36].

29. For these reasons, the EDPB and the EDPS recommend further developing the proposed definition of scientific research[37], by:

    i. moving from Recital 28 to the enacting terms that scientific research should:

        1. be conducted following a methodological and systematic approach of the relevant scientific research field. In addition, it should be added that scientific research should be conducted in an autonomous and independent manner;

        2. lead to verifiable and transparent results. It is recommended to explain in the recitals that transparency may, among other things, involve making research results publicly available. In this regard, it is noted that the publication of the results may also contribute to the aim of contributing to the growth of society's general knowledge and wellbeing.

    ii. moving the phrases 'any research which can also support innovation, such as technological development and demonstration' and '[t]his does not exclude that the research may also aim to further a commercial interest' from the definition into the relevant Recital (insofar as required, taking into account the existing wording in Recital 159 GDPR). The EDPB and the EDPS note that these phrases provide extra context and guidance for the definition of scientific research but do not, as such, constitute criteria for an activity to qualify as scientific research[38]. For example, product research and development may support innovation, but does not necessarily constitute scientific research. Further, providing that scientific research means any research which can also support innovation may unintentionally exclude types of research that do not support innovation but are nevertheless of scientific nature, including fields of research in the humanities or social sciences.

[36] The EU's commitment to scientific research is reflected in the GDPR. By providing specific rules and considerations in this domain, the GDPR provides for a framework that enables and facilitates the processing of personal data for scientific research, while safeguarding the fundamental rights and freedoms of data subjects.

[37] See among others: ALLEA (2023) The European Code of Conduct for Research Integrity – Revised Edition 2023. Berlin. DOI 10.26356/ECOC; World Medical Association (WMA) Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Participants (18th WMA General Assembly, Helsinki, Finland, June 1964, last amended by the 75th WMA General Assembly, Helsinki, Finland, October 2024); Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (ETS No. 164, Oviedo 4.4.1997); Frascati Manual 2015 – Guidelines for Collecting and Reporting Data on Research and Experimental Development (OECD, 2015) (Frascati Manual 2015).

[38] To be clear, the EDPB and the EDPS recognise and agree that scientific research may support innovation and also do not exclude that research may also aim to further a commercial interest, in line also with current Recital 159 GDPR. That being said, the elements of 'technological development and demonstration' or 'furthering a commercial interest' do not constitute useful criteria to differentiate actual scientific research from other forms of research.

4.2 Purpose limitation

30. The EDPB and the EDPS welcome that the Proposal further clarifies the application of Articles 5(1)(b) GDPR and 4(1)(b) EUDPR by providing that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall, in accordance with Article 89(1) GDPR or Article 13 EUDPR, be considered to be compatible with the initial purposes, independent of the conditions of Article 6(4) GDPR or the conditions of Article 6 EUDPR.

31. The EDPB and the EDPS note that current Recital 50 GDPR and Recital 25 EUDPR contain phrases similar to those in Recital 29 Proposal, which provides that '[i]t 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.' [emphasis added] The existing Recitals have not, however, achieved their intended effect of clarifying whether, and under what conditions no legal basis separate from the legal basis for collection of the personal data is required for further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The EDPB and the EDPS therefore recommend to further clarify this in the enacting terms of the GDPR and the EUDPR to ensure legal clarity.

32. The EDPB and the EDPS recall that, in cases where the initial legal basis is relied on for the further compatible processing, the rights of data subjects will then depend on that initial legal basis[39]. The EDPB and the EDPS consider that the fact that data subjects whose data are processed for scientific research may have different rights depending on the initial legal basis relied upon for collection of the data should also be addressed. According to the EDPB and the EDPS, the question of compatibility of purposes should not be confused with the principle of lawfulness under the GDPR and EUDPR.

4.3 Transparency

33. The EDPB and the EDPS support the proposed addition of an Article 13(5) GDPR and Article 15(5) EUDPR. In doing so, the Proposal mirrors the exemption pursuant to Articles 14(5)(b) GDPR and 16(5)(b) EUDPR currently applicable to the provision of information in cases where personal data have not been obtained from the data subject and are processed for scientific research purposes. The EDPB and the EDPS recommend inserting the words 'where and insofar'[40] to ensure that the new provision would extend the same exemption to situations where personal data relating to a data subject were initially collected from the data subject.

34. Provision of information is usually easier in cases of direct collection of personal data. However, there are circumstances under which it is challenging for controllers to inform data subjects individually when personal data are processed for scientific research purposes. For example, this can be the case when personal data that were directly collected from data subjects are further processed for scientific research purposes, but the controller has not retained any contact details. Another example is where the provision of information would render impossible or seriously impair the objectives of scientific research.

---

[39] While some data subject rights apply irrespective of the applicable legal basis, e.g. Articles 16 and 18 EUDPR, some data subject rights apply only in case of applicability of a specific legal basis, see e.g. Articles 20 and 21 GDPR and Articles 22 and 23 EUDPR.

[40] The beginning of the proposed paragraph 13(5) GDPR would then read as follows: 'When the processing takes place for scientific research purposes and **where and insofar as** the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort subject to the conditions and safeguards referred to in Article 89(1)) or in so far as the obligation referred to in paragraph 1 of this Article…' [emphasis added].

4.4 Recital on scientific research and legitimate interest

35. The EDPB and the EDPS support the clarification, in Recital 32 Proposal, that '[t]he processing of personal data for the purpose of scientific research (...) pursues a legitimate interest within the meaning of Article 6(1)(f) [GDPR]', including the important remark that such processing must still comply with the other conditions of Article 6(1)(f) GDPR and other GDPR requirements and principles. For the sake of completeness, the EDPB and the EDPS recommend clarifying in the same Recital that, in some cases, a legal basis under Article 6(1) GDPR other than Article 6(1)(f) GDPR may be appropriate for processing carried out for scientific research purposes.

5 EXEMPTION TO ALLOW THE PROCESSING OF BIOMETRIC DATA

36. The EDPB and the EDPS welcome the proposed introduction of a new derogation from the general prohibition to process special categories of data, limited to situations where processing of biometric data is necessary for the purpose of confirming the claimed identity of a data subject (verification based on a one-to-one comparison)[41]. In particular, the EDPB and the EDPS welcome that this is restricted to cases where the biometric data or the means needed for the verification are under the sole control of the data subject (meaning, in practice, that biometric templates are only stored on a device held by the data subject, such as a badge or smart card, or that biometric templates are stored in a way that makes them unusable without a secret key which is held only by the data subject).

37. In this regard, the EDPB and the EDPS underline that the processing of biometric data, even when it is merely for verification purposes, may only take place in situations where it complies with the necessity and proportionality principles. Therefore, alternative methods not involving the processing of biometric data should be used when the purpose of the processing can be reasonably achieved through less intrusive verification methods in an effective manner, or when the negative impact on the data subjects' fundamental rights and freedoms is not proportional to the anticipated benefits[42]. The EDPB and the EDPS encourage the inclusion of these considerations in the relevant recital[43].

[41] Article 3(3)(a) Proposal, introducing a new letter (l) in Article 9(2) GDPR.
[42] See EDPB Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR, version 1.1, adopted on 23 May 2024, para. 32.
[43] Recital 34 Proposal.

38. The EDPB and the EDPS also recall that the processing of biometric data is currently granted special protection under Article 9 GDPR because of heightened risks to data subjects' rights and freedoms[44]. In that context, they suggest removing the consideration in Recital 34 Proposal, namely 'that processing is not likely to create significant risks to [the data subject]'s fundamental rights and freedoms', since, even if such a processing entails less risks compared to the use of biometric data stored in a centralised database in the clear (or encrypted with a key not solely held by the data subject), it can still imply high risks in some situations, for instance, when biometric data are processed on a large scale. In practice, a data protection risk assessment will in any case be necessary, in accordance with the controller's obligations under the GDPR. The Proposal should instead include examples of appropriate safeguards that controllers should implement when processing biometric data for verification purposes[45].

6 ARTIFICIAL INTELLIGENCE: LEGITIMATE INTEREST AND EXEMPTION TO PROCESS SPECIAL CATEGORIES OF PERSONAL DATA

6.1 Use of legitimate interest in the context of AI models/systems

39. The EDPB and the EDPS agree that, as stated in the first paragraph of proposed Article 88c GDPR, legitimate interest may be used, in some cases, as a legal basis in the context of the development and deployment of AI models or systems. In this regard, the EDPB and the EDPS note that the EDPB has already explicitly confirmed this in its Opinion 28/2024 on AI models[46] on the basis of the current text of the GDPR. Therefore, it is not necessary to add a specific provision to the GDPR on this point – especially in the enacting terms of the text[47]. What is more, the proposed Article 88c simply states that processing in the context of development and operation of AI systems 'may' be pursued for legitimate interests, a statement that does not bring any legal clarification following Opinion 28/2024.

40. Should the co-legislators maintain proposed Article 88c GDPR, first paragraph, in the final text, the EDPB and the EDPS recommend further clarifying the following aspects to fully achieve the objective of ensuring legal certainty and that the applicable conditions are clear for controllers.

[44] Recital 51 GDPR; EDPB Opinion 11/2024, para. 26.
[45] For example, ensuring that when they are stored in a database, the biometric data are encrypted using state of the art algorithms and that the key used to decrypt the data are held only by the data subject; ensuring that end-to-end encryption is used when data are transmitted over a communication channel; providing data subjects with the possibility to securely delete their biometric data at any time. More safeguards are mentioned in EDPB Opinion 11/2024, para. 47, with respect to the situation where the biometric data is under the sole control of the data subject, and para. 61, with respect to the situation where the means needed for the verification are under the sole control of the data subject.
[46] EDPB Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, adopted on 17 December 2024, Section 3.3.
[47] A recital would be more appropriate, see other examples of situations where legitimate interest may be a valid legal basis (e.g., preventing fraud, direct marketing) as provided in Recitals 47 to 49 GDPR.

41. Firstly, as recalled many times by the CJEU and further specified in EDPB Guidelines 1/2024[48], controllers wishing to rely on legitimate interest under Article 6(1)(f) GDPR should carry out a three-step test to assess whether this legal basis is appropriate. The Proposal should expressly refer to the 'legitimate interest' in the first part of the first paragraph of the proposed Article 88c GDPR and state that controllers can only lawfully rely on Article 6(1)(f) GDPR provided that all conditions of that provision are met. This means that, in line with Recital 30 Proposal, controllers still have to carry out the necessary three-step case-by-case assessment to verify that they can lawfully rely on Article 6(1)(f) GDPR. The EDPB and the EDPS also note that the terms 'where appropriate' in the proposed Article 88c GDPR and Recital 30 Proposal decrease rather than increase legal certainty, considering that Article 6(1)(f) GDPR requires a necessity test[49].

42. Secondly, regarding the mitigating measures to implement, the EDPB and the EDPS welcome the reference to an unconditional right to object in Recital 31 and proposed Article 88c, second paragraph GDPR. Nevertheless, instead of creating a new provision in the GDPR, this right should be added to Article 21 GDPR, specifically addressing the situation where processing relies on legitimate interest in the context of the development and operation of AI. The EDPB and the EDPS also recommend clarifying that this right should be brought to the attention of data subjects, when possible and sufficiently in advance of the processing of their personal data, in the context of the development and operation of AI, to enable them to exercise it from the outset[50]. This clarification is necessary, given that it might for instance prove technically difficult to remove personal data that is retained in the AI system or model. In addition, the EDPB and the EDPS consider that the terms 'unconditional right to object' should be further specified, and that Recital 31 should clarify that such a safeguard goes beyond the general right to object set out by Article 21(1) GDPR.

43. Thirdly, 'enhanced transparency' is also mentioned as a mitigating measure[51] without providing clarification on the extent of this transparency obligation. The EDPB and the EDPS recommend clarifying this aspect by specifying that it means providing additional information compared to the information that has to be provided according to Articles 13 and 14 GDPR.

44. Fourthly, the EDPB and the EDPS note that proposed Article 88c, second paragraph GDPR provides a non-exhaustive list of measures to put in place to minimise the risks and impacts for data subjects. However, as previously recalled by the EDPB, mitigating measures should not be confused with the measures that the controller is legally required to adopt to ensure compliance with the GDPR[52], which include for example the data subject rights. The EDPB and the EDPS consider that this aspect should be clarified in the Proposal.

45. Fifthly, to ensure legal clarity, the EDPB and the EDPS recommend defining the term 'operation' [of an AI system], which is neither defined in the GDPR nor in the Artificial Intelligence Act ('AI Act')[53].

[48] EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, version 1.0, adopted on 8 October 2024, para. 6, referring to CJEU caselaw.
[49] EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, p. 12.
[50] In EDPB Opinion 28/2024 on AI models, the EDPB provided some examples of measures that facilitate the exercise of individuals' rights and may be implemented to mitigate the risks identified in the balancing test, see in particular paras. 102(b), 103, and 106.
[51] Recital 31 Proposal and proposed Article 88c GDPR.
[52] EDPB Opinion 28/2024 on AI models, para. 97, referring to EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, adopted on 8 October 2024, para. 57.
[53] 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.

6.2 Additional exemption for incidental and residual processing of special categories of data in the context of the development and operation of an AI system or model

46. The EDPB and the EDPS generally welcome the Proposal's aim to introduce a specific derogation covering the incidental and residual processing of special categories of data in the context of the development and operation of AI systems or models[54], subject to specific conditions[55]. The EDPB and the EDPS appreciate that the proposed Article 9(5) GDPR aims at avoiding the collection and processing of special categories of personal data and at introducing specific safeguards in case that said processing cannot be avoided. In this respect, the EDPB and the EDPS acknowledge that when collecting data for the training, testing and validation of certain AI systems or models (e.g. a general-purpose AI model), it is not always possible for controllers to avoid residual and incidental processing of special categories of data[56].

47. In order to ensure legal certainty for data subjects, as well as for developers and providers of certain AI systems or models, and taking into account the risks arising from the residual and incidental processing of special categories of personal data, the EDPB and the EDPS suggest some improvements to the current Proposal.

48. The EDPB and the EDPS recall that the processing of personal data should be done in accordance with the principles laid down in the GDPR and be necessary and proportionate to the purposes of the processing. Against this background, the proposed Article 9(2)(k) GDPR, read in conjunction with the proposed Article 9(5) GDPR and Recital 33 Proposal, addresses the situation where the main processing operation leads to an incidental and residual processing of special categories of personal data. Therefore, where the processing of special categories of personal data is necessary for the purposes of the processing in the context of the 'development and operation' of AI systems or models, the derogation will not apply and data controllers will need to rely on another derogation under Article 9(2) GDPR, if applicable[57]. The EDPB and the EDPS recommend that the reference to the 'incidental and residual' processing is added in the enacting terms, in order to ensure the correct interpretation of the proposed Article 9(2)(k) GDPR.

49. Furthermore, the EDPB and EDPS recommend clarifying the scope of the proposed Article 9(2)(k) GDPR. The EDPB and the EDPS note that, while the proposed Article 9(2)(k) GDPR refers to the development and operation of an AI system or model, Recital 33 Proposal only refers to the incidental and residual processing of special categories of data in the context of the development of AI systems or models. Taking this into account, as well as the lack of definition of the concept of 'operation'[58], the EDPB and the EDPS highlight that the scope of the proposed Article 9(2)(k) GDPR should not be understood as covering the processing of special categories of personal data collected through prompts during the deployment of the AI system or model. Therefore, the EDPB and the EDPS recommend clarifying the scope of the derogation.

[54] With respect to the use of the term 'operation', the EDPB and the EDPS refer to their recommendation in paragraph 45 of this Joint Opinion.
[55] Articles 3(3)(a) and (b) Proposal, adding a new letter (k) to Article 9(2) GDPR and a new paragraph 5.
[56] Articles 3(3)(a) and (b) Proposal, adding a new letter (k) to Article 9(2) GDPR and a new paragraph 5.
[57] See Recital 33 Proposal.
[58] See paragraph 45 of this Joint Opinion.

50. Moreover, the proposed Article 9(5) GDPR should explicitly include a precondition that deletion of the personal data that is subject to the derogation in proposed Article 9(2)(k) GDPR is impossible or involves disproportionate efforts. Additionally, the proposed Article 9(5) GDPR should indicate that the controllers' assessment has to be based on a properly documented effort, considering the state-of-the-art technology and the impact on data subjects.

51. Finally, the EDPB and the EDPS suggest emphasising, in the proposed Article 9(5) GDPR, that safeguards should be implemented across the AI development lifecycle to ensure the effective protection of the special categories of data when their deletion would be impossible or entail a disproportionate effort. In addition, the text could clarify that the effective protection also includes the need to prevent the re-use of those data for other purposes. The EDPB and the EDPS recommend adding this element as well in the last sentence of the proposed Article 9(5) GDPR.

52. The EDPB and the EDPS understand that the proposed Article 4a AI Act, introduced under the new AI Omnibus Proposal[59], would have a more limited scope and would apply only to a specific dataset of special categories of data processed intentionally for the sole purpose of bias detection and correction. To avoid any confusion between the respective regime for the processing of special categories of data under both provisions, the EDPB and the EDPS therefore recommend clarifying the interplay between both provisions and to clearly delineate the scope of the proposed Article 9(2)(k) GDPR as suggested above. In addition, the EDPB and the EDPS invite the co-legislators to consider adding a cross reference to each provision in the corresponding Recitals, explaining the difference of scope, regime and conditions for both processing.

7 RIGHTS OF DATA SUBJECTS

7.1 Limitation to data subject access requests

53. With respect to the amendments to Article 12(5) GDPR, the EDPB and the EDPS agree with the Commission's aim to provide legal clarity to controllers in situations where there is an abuse of rights[60], as it reinforces the consistent application of the GDPR.

54. However, the EDPB and the EDPS consider that part of the proposed wording is problematic where it links the notion of abuse of rights with the exercise of the rights for purposes other than the protection of personal data. In this respect, the EDPB and the EDPS recall that Article 1 GDPR explicitly calls for the protection of 'natural persons with regard to the processing of their personal data' and of 'fundamental rights and freedoms of natural persons and *in particular* their right to the protection of personal data' [emphasis added]. This provision clearly underlines that the GDPR, and more generally the right to protection of personal data in Article 8 of the Charter, aims to protect all individuals' fundamental rights and freedoms, and is not limited to the protection of personal data alone. This has been already confirmed by the CJEU, which considers that data subjects may legitimately exercise their right to access also for objectives 'other than that of becoming aware of the processing of data and verifying [its] lawfulness' (and without having to provide any particular motivation)[61].

[59] Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) ('the AI Omnibus Proposal').
[60] Commission Staff Working Document, section 1.2.2.5.
[61] Judgment of the CJEU of 26 October 2023, Case C-307/22, ECLI:EU:C:2023:811, paragraphs 38 and 43.

55. Therefore, the EDPB and the EDPS consider that the future legislation should refrain from linking the notion of abuse of rights with the exercise of the right to access for purposes other than data protection. Rather, it should link the notion of 'abusive requests' with the existence of an abusive intention[62] (e.g., evident intention to cause harm to the controller).

56. With respect to the references to 'unfounded' and 'excessive' access requests in Recital 35 Proposal, the EDPB and the EDPS recommend removing the consideration that 'overly broad and undifferentiated requests should be regarded as excessive'. That statement runs counter to the main objective of the right of access, which is to enable data subjects to be aware of the processing concerning them[63]. Recital 63 GDPR already takes into account situations where controllers are processing large volumes of personal data, as it allows controllers to request that the data subject specifies the information or processing activities concerned by their request[64]. In a similar vein, the EDPB and the EDPS recommend that the future legislation specifies that, if an assessment of objective elements by the controller shows that a request is manifestly unfounded, the data subject should be provided with the opportunity to further specify their request.

57. Furthermore, the EDPB and the EDPS consider that the proposed changes in the last sentence of Article 12(5) GDPR regarding the threshold of the burden of proof should be reconsidered and that the current threshold for the assessment of both excessive and manifestly unfounded requests be maintained, in order to limit the possibility of misuse by controllers. In particular, the EDPB and the EDPS have doubts that the inclusion of the notion of 'reasonable grounds to believe' would actually maintain the same high level of protection for individuals or achieve the objective of simplification, and recommend removing it.

58. Recital 35 Proposal should also be amended to clarify that the assessment of the excessive or manifestly unfounded character of a request should be properly documented and based on an objective assessment. Further, it should be clarified that the data subject should have the opportunity to provide clarifications before the request is rejected.

[62] See Judgement of the CJEU, Case C-307/22, paragraph 31. See also Opinion of Advocate General Szpunar of 18 September 2025, Case C-526/24, *Brillen Rottler*; ECLI:EU:C:2025:723, paragraph 41 (according to which an access request can be considered excessive when the controller demonstrates, in light of all relevant circumstances of the case, an abusive intention on the part of the data subject) and Judgement of the CJEU of 9 January 2025, Case C-416/23, *Österreichische Datenschutzbehörde*,, ECLI:EU:C:2025:3, paragraph 56. See also EDPB Guidelines 01/2022 on data subject rights Right of access, version 2.1, adopted on 28 March 2023, paragraphs 188 and 190.

[63] Recital 63 GDPR.

[64] See also EDPB Guidelines 01/2022 on data subject rights - Right of access, Version 2.1, Adopted on 28 March 2023, para. 35.

59. Finally, the EDPB and the EDPS note that a controller's ability to refuse to handle a data subject's request or to charge a reasonable fee enshrined in Article 12(5) GDPR is currently mirrored in Article 57(4) GDPR, which provides supervisory authorities with equivalent possibilities in relation to complaints. The EDPB and the EDPS consider that supervisory authorities should also be able to refuse to act on a complaint or should be able to charge a reasonable fee under the same conditions as a controller would be able to refuse to grant a request for access. Article 57(4) GDPR could therefore be amended accordingly, provided that the remarks set out in this section on Article 12(5) GDPR are duly taken into account. This change would lead to a more efficient use of resources by supervisory authorities and faster resolutions for complainants overall. More generally, the EDPB and the EDPS urge the co-legislators to duly take into account the issue of the adequacy of human and financial resources of supervisory authorities[65], also considering the increase of the number of complaints[66] and of the competences and tasks entrusted to supervisory authorities under the EU digital legislation.

7.2 Transparency: Exemption to the provision of information where personal data are collected from the data subject

60. The EDPB and the EDPS welcome the objective of simplifying information requirements and reducing administrative burden, in particular for SMEs, including by derogating from the duty to provide information in cases where the data subject has it readily available. Therefore, the EDPB and the EDPS agree with modifying Article 13(4) GDPR in this direction.

61. At the same time, the EDPB and the EDPS note that the proposed modified wording of Article 13(4) GDPR may lead to uncertainty and divergent interpretations. The EDPB and the EDPS recommend maintaining carefully limited and clearly defined conditions in Article 13(4) GDPR, also in light of the principle of proportionality, to ensure that the new exemption to the provision of information effectively leads to a reduction of the administrative burden for controllers.

62. First, the EDPB and the EDPS recommend further clarifying the concepts of 'not data-intensive activity' and 'clear and circumscribed relationship'. These concepts still appear ambiguous, and thus would not attain the intended objectives of clarity and simplification, despite the examples provided in Recital 36 Proposal. In particular, the notion of 'not data-intensive activity' may refer both to the quality and the quantity of personal data being processed. Also, as explained in paragraph 57 above, the EDPB and the EDPS have doubts that the inclusion of the notion of 'reasonable grounds to assume' would actually maintain the same high level of protection for individuals or achieve the objective of simplification, and recommend removing it. It should also be clarified that the assessment should rely on objective elements.

63. Secondly, the EDPB and the EDPS recommend including in the provision that the controller would still be required to provide all information listed by Article 13 GDPR upon request by the data subject, and that the data subject should be informed about this possibility. If data subjects are not able to obtain information pursuant to Article 13 GDPR upon request, they would be left only with the possibility to file access requests pursuant to Article 15 GDPR[67].

[65] Article 52(4) GDPR requires Member States to ensure that each SA is provided with the resources necessary for the effective performance of its tasks and exercise of its powers. The CJEU underlined that those resources must be adapted to the use that data subjects make of their right to lodge complaints, and that Member States need to provide SAs with the appropriate resources to process all complaints submitted to them, if necessary by increasing those resources in the light of the use made by data subjects of their right to lodge complaints (Judgment of the Court of Justice of 9 January 2025, Case C-416/23, Österreichische Datenschutzbehörde v F R, ECLI:EU:C:2025:3, paras. 51-52).

[66] See in this regard the Commission's Second Report on the application of the General Data Protection Regulation, COM/2024/357 final, section 2.5.2 ('Difficulties handling a high number of complaints').

[67] Recital 36 Proposal.

64. Finally, the EDPB and the EDPS note that the proposed amendment to Article 13(4) GDPR is not reflected in the proposed changes to EUDPR. To ensure consistency, the EDPB and the EDPS recommend the co-legislators to align Article 15(4) EUDPR with the amended version of Article 13(4) GDPR, taking into account the position expressed by EDPB and the EDPS on this matter.

7.3 Automated individual decision-making

65. The EDPB and the EDPS note that the Proposal would change Article 22(1) GDPR and Article 24(1) EUDPR from a 'right not to be subject to' automated decision-making that produces legal effects for the data subject or similarly significantly affects them to a provision laying down the exhaustive list of cases where such types of decisions are permitted.

66. The EDPB and the EDPS recall that the CJEU has interpreted Article 22(1) GDPR as a prohibition in principle, the infringement of which does not need to be invoked individually by the data subject[68]. Therefore, the EDPB and the EDPS consider it necessary to use appropriate language to reflect that Article 22(1) GDPR and Article 24(1) EUDPR provide for prohibitions with exceptions under specific conditions, as clarified by the CJEU. An appropriate wording to this effect could be that 'a decision which produces legal effects for a data subject or similarly significantly affects them shall not be based solely on automated processing, including profiling, unless that decision: (...).' This would prevent that the possibilities for relying on automated decision-making with particularly serious impacts on data subjects are interpreted too broadly, thereby retaining a high level of protection for individuals that is necessary in light of the potential risks involved for their interests and rights[69].

67. Furthermore, the EDPB and the EDPS recommend that Recital 38 Proposal explicitly clarifies that Article 22(1) GDPR and Article 24(1) EUDPR would continue to also provide a right that data subjects can invoke[70], in addition to the rights and safeguards provided under Article 22(3) GDPR and Article 24(3) EUDPR[71]. In this context, it should be noted that Article 22 remains under Chapter III GDPR, which has as its title 'rights of the data subject'.

68. The Proposal also aims to clarify the first among the conditions that would legitimise automated decision-making captured by Article 22(1) GDPR and Article 24(1) EUDPR, namely where automated decision-making is necessary for entering into or performing a contract between the data subject and a data controller. According to the Proposal, the necessity of the (automated) decision should be assessed without consideration of whether the decision could be taken otherwise than by solely automated means. Recital 38 Proposal specifies 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'.

69. The EDPB and the EDPS welcome this objective of clarification as this may also lead to more consistency of application of Article 22(1) GDPR and Article 24(1) EUDPR. The EDPB and the EDPS understand that the main intent of the Proposal is not to change the derogation under current Article 22(2)(a) GDPR and Article 24(2)(a) EUDPR *per se*, but merely to clarify that the requirement of necessity does not mean that the mere fact that a decision could theoretically also be taken by a human should prevent the controller from taking the decision by solely automated means.

---

[68] Judgment of the Court of Justice of 7 December 2023, C-634/21, *SCHUFA Holding*, ECLI:EU:C:2023:957, paragraph 52.
[69] Recital 71 GDPR.
[70] Recital 71 GDPR.
[71] Such as the obligation to implement suitable measures to safeguards the rights of the data subjects 'rights and freedoms and legitimate interests, to obtain human intervention on the part of the controller and to express their view and to contest the decision.

70. In this context, the EDPB and the EDPS consider that the combination of the words 'necessary' and 'regardless of whether the decision could be taken otherwise than by solely automated means' in Articles 3(7) and 4(6) Proposal might create confusion in the interpretation and application of the derogation.

71. In any event, processing must be necessary to conclude or perform a contract, as already laid down in Article 6(1)(b) GDPR[72]. This provision, together with the principle of data minimisation provided by Article 5(1)(c) GDPR, remains applicable regardless of whether Article 22 GDPR applies, and therefore obliges controllers to choose the least intrusive among the equally effective processing options at their disposal.

72. Therefore, the EDPB and the EDPS recommend amending the Proposal to avoid giving the wrong impression that automated decision-making is in principle allowed whenever available in the context of a contract despite the use of the word 'necessary'. This could be achieved by keeping the clarification 'regardless of whether the decision could be taken otherwise than by solely automated means' only in Recital 38, but not in the enacting terms of the text. Moreover, the last sentence of Recital 38 should be amended to clarify that automated decision-making covered by Article 22(1) GDPR and Article 24(1) EUDPR is only 'necessary' if no other equally effective and less intrusive means (automated or not) are available to the controller[73].

8 DATA BREACHES

8.1 Notifications

On the increase of the threshold to notify data breaches:

73. The EDPB and the EDPS support the Proposal's increase of the threshold for controllers to notify data breaches to the competent supervisory authorities. This change is not expected to substantially affect the level of protection for data subjects but would significantly reduce the administrative burden for controllers, given that they would only have to notify data breaches that are likely to result in a high risk to the rights and freedoms of data subjects.

74. In any case, the EDPB and the EDPS recall that, in line with Article 33(5) GDPR, controllers shall document *any* personal data breaches and that this shall enable the competent supervisory authority to verify controller's compliance with the notification obligation.

75. In addition, the increase in the notification threshold does not affect the controller's obligation to comply with Article 32 GDPR, including the obligation to implement appropriate measures to mitigate possible adverse effects of a personal data breach.

[72] See, in this regard, Judgment of the Court of Justice of 12 September 2024, Joined Cases C-17/22 and C-18/22, *HTB Neunte*, ECLI:EU:C:2024:738, paragraphs 43 and 44.

[73] See Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, last revised and adopted on 6 February 2018 and endorsed by the EDPB on 25 May 2018. On page 23, the Article 29 Data Protection Working Party clarified that controllers need to be able to 'show that [the] processing [covered by Article 22(1) GDPR] is necessary taking into account whether a less privacy-intrusive method could be adopted'.

76. The EDPB and the EDPS also support the proposal to raise the threshold for the reason that some supervisory authorities face a large number of data breach notifications (up to thousands of notifications per year[74]), including minor ones[75]. Therefore, this new threshold could help supervisory authorities by allowing them to focus resources on the more problematic data breaches, ultimately benefiting data subjects affected by those breaches.

On the extension of the deadline to notify data breaches:

77. The EDPB and the EDPS support extending the deadline for controllers to notify a data breach, from 72 to 96 hours, after having become aware of the breach[76]. This change is not expected to substantially affect the level of protection for data subjects. In addition, the current deadline of 72 hours may be challenging as it may include weekends and bank holidays. This is particularly difficult for smaller organisations, especially SMEs. In addition, in line with Article 33(4) GDPR, some controllers notify data breaches in a layered manner, providing a first set of available information by the legal deadline and the remaining required information through a second complementary notification. Therefore, the proposed extension would lighten the administrative burden for notifying controllers by giving them one more day to gather the relevant information and improve the quality of the notification, while using the extra time to already implement remediation measures.

78. The positive effects of this change on controllers could also indirectly benefit data subjects, with supervisory authorities receiving more complete and accurate information, and remediation measures possibly implemented even before the notification.

79. The EDPB and the EDPS nevertheless underline the fact that shorter deadlines apply under other reporting obligations[77], namely: NIS2 Directive[78] (24 or 72 hours depending on the obligation), DORA[79] (24 or 72 hours depending on the obligation), eIDAS Regulation[80] (24 hours) and CER Directive[81] (24 hours). The EDPB and the EDPS would recommend more harmonisation between the different notification obligations. This is all the more important since one of the purposes of the single-entry point, as assessed below, is to allow 'to seemingly file one single notification, whereas responding to multiple legal obligations at the same time'[82].

[74] For instance, in 2025, the DK SA received 9,302 notifications (https://www.datatilsynet.dk/sikkerhedsbrud/statistik-over-brud-paa-persondatasikkerheden/antal-anmeldte-brud). In 2024, the IE SA received 7,781 valid breach notifications (https://www.dataprotection.ie/annualreport2024/), while the NO SA received 3,191 notifications (https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/datatilsynets-arsrapporter/arsrapport-for-2024/utvalgte-hovedtall/).

[75] European Agency for Fundamental Rights (FRA), GDPR in practice, Experiences of data protection authorities, 11 June 2024, section 1.1, p. 20.

[76] In any event, the EDPB and the EDPS note that under the proposed Article 34(1) GDPR, controllers would still be required to notify the data breach '*without undue delay* and, where feasible not later than 96 hours after having become aware of it (...)' (emphasis added).

[77] Article 23a(3)(f) Proposal.

[78] Article 23 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive), OJ L 333, 27.12.2022, pp. 80–152.

[79] Article 19 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA), OJ L 333, 27.12.2022, pp. 1–79 and Article 5 of Commission Delegated Regulation (EU) 2025/301 of 23 October 2024 supplementing DORA with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats.

[80] Article 19 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation), OJ L 257, 28.8.2014, pp. 73–114.

[81] Article 15 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (CER Directive), OJ L 333, 27.12.2022, pp. 164–198.

[82] Proposal, COM(2025) 836 final, Explanatory Memorandum, section 2, 'Subsidiarity (for non-exclusive competence), p.10.

8.2 Common EDPB template and list of circumstances

80. The EDPB and the EDPS support the proposed obligation for the EDPB to prepare both a common template for notifying data breaches and a list of circumstances in which a data breach is likely to result in a high risk. These changes are expected to positively benefit the level of protection of data subjects due to the increased consistency and can simplify the compliance efforts of controllers.

81. The proposed template would also be fully in line with the EDPB Helsinki Statement, in which the EDPB announced that it would draft such a template in view of streamlining data breach notifications and easing the burden of organisations, in support of a possible cross-regulatory European notification solution. The common template and the list of circumstances would be consistent with Pillar 1 of the EDPB Strategy 2024–2027[83], as they would facilitate compliance, including for SMEs. The proposed list of circumstances would further harmonise the notion of 'likely to result in a high risk to the rights and freedoms of data subjects' and help controllers to better assess risks following a data breach.

82. However, the Proposal entrusts the Commission with the review and the unilateral modification of the template and the list prepared by the EDPB when adopting them by way of an implementing act[84]. In that regard, the wording 'after due consideration reviews it' leaves too much discretion for the Commission regarding the extent to which the proposed documents from the EDPB will be reviewed and taken into account[85]. Amongst other issues, this procedure does not entail a consultation of the EDPB on the changes possibly introduced by the Commission. Instead, the EDPB and the EDPS recommend entrusting the EDPB with the preparation and approval of the template and the list. This would be similar, for example, to the power already entrusted to the EDPB to approve certification criteria resulting in the European Data Protection Seal[86].

83. Strengthening the role of the EDPB in such a way would ensure that the process is still assigned to an independent body, and would more closely follow the principle of subsidiarity, than if it were implemented by the Commission, as the EDPB is composed by national supervisory authorities. In addition, it would be more likely to efficiently leverage on the supervisory authorities' expertise on the enforcement of these provisions.

84. The EDPB and the EDPS stress that the revision of the EUDPR should also provide for the establishment of a common template for notifying personal data breaches, as well as for the establishment of a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person. The competence to establish such template and list should be entrusted to the EDPS. As to the EUDPR, the EDPS is already empowered to adopt lists of processing activities requiring and not requiring DPIAs. The EDPB and the EDPS consider that transferring this responsibility to the Commission is not necessary, nor appropriate, given that the Commission would itself have to comply with those lists. The Commission, as a European institution should not be given the possibility of shaping the extent of its own obligations under the EUDPR.

[83] EDPB Strategy 2024-2027, April 2024.
[84] Article 3(8)(c) Proposal.
[85] Article 3(8)(c) Proposal, adding Article 33(6) and 33(7) GDPR refers to 'after due consideration'.
[86] Article 42(5) GDPR. Also see below Section 9.1 on the adoption procedure of the common EDPB DPIA whitelist and blacklist.

8.3 Single-entry point (SEP)

85. The EDPB and the EDPS strongly support the objective of the establishment of the single-entry point ('SEP') pursuant to Article 23a of Directive (EU) 2022/2555 for the notification of personal data breaches, as it would reduce the administrative burden for organisations without affecting the level of protection for data subjects. An EEA-wide SEP is welcome, as it will make it easier for organisations to fulfil their different reporting obligations in the event of a security incident. In its EDPB Helsinki Statement, the EDPB already underlined its support for a possible cross-regulatory European notification solution as this would help make GDPR compliance easier.

86. The EDPB and the EDPS highlight the importance of ensuring the security of the notifications submitted to and transmitted through the SEP, as data breach notifications often include sensitive information.

87. The EDPB and the EDPS further consider that Article 34(1) EUDPR should also include provisions mirroring the modifications proposed under Article 33(1) GDPR, in particular to allow EUIs to notify data breaches through the single-entry point.

9 DATA PROTECTION IMPACT ASSESSMENT

9.1 Common EDPB DPIA lists

88. The EDPB and the EDPS support the harmonisation at EU level introduced by the Proposal with regard to the lists of data protection impact assessment ('DPIA') under Articles 35(4) and 35(5) GDPR. While the consistency mechanism[87] already serves its purpose, the introduction of common EEA lists would further harmonise and bring further clarity as to whether a DPIA is required or not and reduce businesses' compliance burden, in alignment with the EDPB Helsinki Statement.

89. The EDPB and the EDPS note that the Proposal affects the role and prerogatives currently entrusted to supervisory authorities under the GDPR with regard to the establishment of DPIA lists[88]. In this regard, the EDPB and the EDPS support the assignment of a new role, to propose such lists, to the EDPB[89] but recommend further strengthening it.

90. The Proposal entrusts the Commission with the unilateral modification of the lists prepared by the EDPB when adopting them by way of an implementing act[90]. In this regard, the EDPB and the EDPS express the same concerns as for the proposed implementing acts on data breaches (see paragraphs 82 and 83 of this Joint Opinion)[91]. The EDPB and the EDPS therefore suggest entrusting the EDPB exclusively with the preparation and approval of DPIA lists with general validity within the Union, for the same reasons as expressed in paragraphs 82 and 83.

[87] As set out in Chapter VII, section 2 GDPR.
[88] The Proposal deletes the current Articles 57(1)(k) and 64(1)(a) GDPR.
[89] Articles 3(9)(a), 3(9)(b) and 3(14) Proposal. According to the Proposal, the EDPB would have the role of preparing the DPIA lists and assessing the possible need of updates at least every three years, while the Commission would review and adopt the DPIA lists prepared by the EDPB (and any updates) via an implementing act.
[90] Article 3(9)(b) Proposal.
[91] In this regard, the EDPB notes that Article 3(9)(b) Proposal, adding Article 35(6a) and 35(6b) GDPR, also refers to 'after due consideration reviews it' and is subject to the same criticism as the use of the language in Article 3(8)(c) Proposal, adding Article 33(6) and 33(7) GDPR.

91. The EDPB and the EDPS note that the proposed amendment to Article 39 EUDPR is neither necessary (as it is not required to achieve the goal of harmonisation), nor appropriate (as it would affect the independence of the process leading to the establishment of the lists of processing activities subject or exempted from a DPIA under the EUDPR)[92]. The EDPS is already empowered to adopt lists of processing activities requiring and not requiring DPIAs that apply to all EUIs. When developing those lists, the EDPS can ensure consistency with the ones developed under the GDPR. The EDPB and the EDPS therefore recommend the co-legislators not to adopt the amendments proposed under Article 39 EUDPR.

9.2 Common EDPB template and methodology for DPIA

92. The EDPB and the EDPS welcome the proposed creation of a common template and a common methodology for conducting data protection impact assessments as it can simplify the carrying out of this important process by organisations. As a follow-up of the EDPB Helsinki Statement, the EDPB had already announced that it will draft such a template to be used across the EEA.

93. With regard to the methodology for conducting a DPIA, the EDPB and the EDPS suggest clarifying that this concept should be understood in a broad and practical sense, resulting in a guided process and principles to be applied and not simply a mere documentation or checklist exercise. Such a clarification would allow the flexibility needed due to the contextual diversities and the diverse types of processing operations it could be applied to. Moreover, referring to a methodology for conducting a DPIA in a broad and practical sense would allow the continued use, and adaptations only if necessary, of existing methodologies and technological tools which are already widely used by organisations.

94. The EDPB and the EDPS also suggest modifying the allocation of powers envisaged in the Proposal and strengthening the role of the EDPB, for the same reasons developed in paragraphs 82 and 83 of this Joint Opinion. The attribution of this new task to the EDPB is also aligned with the Helsinki Statement and the EDPB's ongoing work to develop new tools to make GDPR compliance easier.

95. The EDPB and the EDPS recommend that the proposed revision of the EUDPR provides for the introduction of a common methodology to be followed by EUIs for conducting data protection impact assessments. The EDPB and the EDPS recommend, however, that such methodology be adopted by the EDPS. Empowering the Commission to adopt the methodology is neither necessary nor appropriate, for the same reasons as the ones mentioned above in paragraph 90.

[92] In this regard, it is worth noting that the Commission, as a European institution would be given the possibility of shaping the extent of its own obligations under the EUDPR if it were able to define the precise circumstances in which a DPIA under the EUDPR would (not) be required.

10 EPRIVACY PROVISIONS: PROTECTION OF TERMINAL EQUIPMENT AND SECURITY OF PROCESSING

10.1 Changes to the protection of information stored or accessed in terminal equipment

General

96. The EDPB and the EDPS strongly support the aim of the Proposal to provide for a regulatory solution on consent fatigue and proliferation of cookie banners and to simplify the rules applicable to the protection of the terminal equipment of end-users. The EDPB and the EDPS also generally welcome that the Proposal aims to provide limited additional derogations to the general prohibition to store or gain access to personal data in the terminal equipment (subject to further remarks below) and the fact that the oversight of such matters will be entrusted to the supervisory authorities established in accordance with Article 51 GDPR to further support regulatory consistency[93].

97. Pursuant to the Proposal, the protection of terminal equipment would be covered by the GDPR and EUDPR on the one hand, and the ePrivacy Directive[94] on the other hand, introducing two different regimes depending on whether the data are personal or non-personal in nature. The EDPB and the EDPS consider that the envisaged aims of simplification, legal certainty, and – with regard to the GDPR[95] – bringing the provision under the supervision of one authority[96], may be not achieved for the following reasons:

    i. information stored in the terminal equipment may include personal data and non-personal data, which may lead to uncertainty as to which rules apply to a particular operation (e.g., the processing of personal data under the GDPR and EUDPR might be able to rely on an exception to consent (pursuant to Article 88a (3) GDPR), while consent would be necessary under the ePrivacy Directive for the processing of non-personal data);

    ii. it would require a systematic and objective analysis by those involved (which may in some cases be numerous) in the storing or accessing information whether it concerns personal data or not, and they may be uncertain (or disagree) as to which legal framework applies;

[93] As a consequence, all supervisory authorities will become competent for the oversight of this provision and the cooperation and consistency mechanism will also apply in this regard. See also EDPB Statement on the ePrivacy Regulation and the future role of Supervisory Authorities and the EDPB, adopted on 19 November 2020, p. 2 ('In order to ensure a high level of protection of personal data and to guarantee legal and procedural certainty, this oversight should be entrusted to the same national authorities, which are responsible for enforcement of the GDPR as initially proposed by the European Commission') and EDPB Statement 03/2021 on the ePrivacy Regulation, adopted on 9 March 2021, p. 4-5 ('Provisions of the future ePrivacy Regulation related to the protection of privacy should not be applied in isolation, since they are intertwined with personal data processing and the GDPR. Hence, in order to conciliate a high level of protection of personal data and legal and procedural certainty, national authorities responsible for enforcement of the GDPR should be entrusted with the oversight of the provisions of the future ePrivacy Regulation related to the processing of personal data, as initially proposed by the European Commission').

[94] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, pp. 37–47.

[95] Under the EUDPR, the EDPS is already competent to supervise the protection of information transmitted to, stored in, related to, processed by and collected from users' terminal equipment. Article 37 EUDPR provides that 'Union institutions and bodies shall protect the information transmitted to, stored in, related to, processed by and collected from the terminal equipment of users accessing their publicly available websites and mobile applications, in accordance with Article 5(3) of Directive 2002/58/EC.'

[96] Proposal, COM(2025) 836 final, Explanatory Memorandum, p. 7.

iii. the protection of terminal equipment would potentially remain subject to supervision by different authorities, namely supervisory authorities under the GDPR, and other regulators that would be or remain competent to supervise Article 5(3) ePrivacy Directive[97].

98. The EDPB and the EDPS recall that the purpose of current Article 5(3) ePrivacy Directive is to implement not only the right to the protection of personal data (Article 8 of the Charter), but also the fundamental right to respect for private life and communications (Article 7 of the Charter).

Subsequent processing

99. New Proposed Article 88a(3) GDPR and Article 37(4) EUDPR provide that 'storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and *subsequent processing*, shall be lawful (...)' [emphasis added]. This means that these two proposed provisions regulate not only the lawfulness for storage of and access to personal data in terminal equipment, but also the lawfulness of subsequent processing. The EDPB and the EDPS understand this to concern the processing operations following the storing of or gaining of access to personal data for the same purpose as for which personal data was stored or accessed in the terminal equipment[98]. For the sake of clarity, the EDPB and the EDPS recommend to also refer to 'purposes' in the enacting terms of the Proposal[99].

100. The EDPB and the EDPS note that proposed Article 88a(1) and (2) GDPR and proposed Article 37(2) and (3) EUDPR take a different approach than Article 88a(3) GDPR and Article 37(4) EUDPR, as the former do not regulate the lawfulness of *subsequent processing*. To ensure legal certainty and to simplify compliance, the EDPB and the EDPS recommend to regulate the subsequent processing of personal data accessed or stored in terminal equipment based on consent or Union or Member State law[100] in a similar manner as under proposed Articles 88a(3) GDPR and 37(4) EUDPR[101]. This would entail that subsequent processing of personal data stored or accessed in terminal equipment, for the *same* purpose, would rely on the same consent or provision of Union or Member State law allowing the personal data to be initially stored or accessed. Proposed Recital 44 should also be amended accordingly, also clarifying that where processing relies on consent under Article 88a(1) GDPR and Article 37(2) EUDPR, the consent should clearly encompass both the access to the terminal equipment and the subsequent processing carried out for the same purpose. Subsequent processing of personal data for a purpose other than that for which the personal data has been stored or accessed will be considered as further processing, as referred to under Article 6(4) GDPR[102].

Exceptions to consent

[97] It is noted that different than for the GDPR, the supervision of both Article 37(1) EUDPR - which provides that Article 5(3) ePrivacy Directive applies - and proposed Article 37(2)-(6) EUDPR is under the competence of the EDPS. The designation of the authorities responsible for the oversight of the ePrivacy Directive is left to the decision of Member States. Therefore, supervisory authorities may be competent to enforce Article 5(3) of the ePrivacy Directive in some Member States, while other authorities are competent in other Member States.

[98] This is already implied in Recital 44 Proposal, which states that 'For the subsequent processing of personal data for other purpose than those defined in the limitative list, Article 6 and, where relevant, Article 9 of Regulation (EU) 2016/679 should be applied.'

[99] In particular by adding in proposed Article 88a(3) GDPR the word 'purposes' after the word 'following'.

[100] I.e. pursuant to proposed Article 88a(1) and (2) GDPR and proposed Article 37(2) and (3) EUDPR

[101] On the lawfulness of subsequent processing, see e.g. EDPB Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, adopted on 9 March 2021, para. 15; EDPB Guidelines 8/2020 on the targeting of social media users, adopted on 13 April 2021, para. 78; and EDPB Guidelines 02/2021 on virtual voice assistants, adopted on 7 July 2021, para. 27.

[102] See also EDPB Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, adopted on 9 March 2021, para. 15 and EDPB Guidelines 8/2020 on the targeting of social media users, adopted on 13 April 2021, footnote 38.

101. The EDPB and the EDPS note that compared to current Article 5(3) ePrivacy Directive, proposed Article 88a(3)(b) GDPR and proposed Article 37(4)(b) EUDPR contain a broadened exception to consent for access to storage of personal data in terminal equipment. Namely, pursuant to the Proposal, no consent is required for 'providing a service explicitly requested by the data subject', while under Article 5(3) ePrivacy Directive, this exception is limited to the provision of an *information society* service. In addition, proposed Article 88a(3)(c)–(d) GDPR and proposed Article 37(4)(c)–(d) EUDPR contain new exceptions for audience measurement and security purposes accordingly[103]. In this regard, the EDPB and the EDPS recommend to clearly delimit the processing in scope of such exceptions to what is strictly necessary.

102. To ensure legal certainty, it should be specified that creating aggregated information about the usage of an online service to measure the audience of such a service where it is carried out by the controller of that online service solely for its own use ('audience measurement') means processing to obtain insight into the performance and use of the online service in an aggregated and general manner (i.e. the aggregated information should not relate to a specific data subject, i.e. be anonymous aggregated information). The data collected should not be further processed for another purpose, combined with data from other services from the provider of the online service or from a third party (e.g. analytics information from other websites or apps), or shared with third parties[104]. The EDPB and the EDPS also recommend clarifying that data may be collected either by a provider[105] of an online service solely for its own use, or by a processor acting on behalf of this provider.

103. In addition, proposed Article 88a(3)(d) GDPR regarding lawfulness of processing for maintaining or restoring the security of a service should be further specified to mean IT security and data protection security[106]. The EDPB and the EDPS fully support the objective of the Proposal as there is a legitimate interest in ensuring that the security of a service or terminal equipment remains up-to-date. A provider of security patches should in general therefore be able to install the strictly necessary security updates without consent from the user. However, this should only be allowed to the extent that (i) the security updates are discretely packaged and do not in any way change the functionality of the software on the terminal equipment (including the interaction with other software or settings chosen by the user), (ii) the end-user is informed in advance each time an update is being installed, and (iii) the user has the possibility to turn off the automatic installation of these updates.

[103] Pursuant to the Proposal, no consent is required for 'creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use' and 'maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service'. No such exceptions are provided under Article 5(3) ePrivacy Directive.
[104] See WP 194, Opinion 04/2012 on Cookie Consent Exemption, adopted on 7 June 2012, p. 10-11.
[105] The notion 'controller' relates to the processing of personal data, rather than to the provision of a service, which appears to be what the exception intends to refer to.
[106] Examples are inter alia detecting repeated failed login attempts on a website or protecting the login system from misuse.

104. The EDPB and the EDPS also suggest that the co-legislators consider introducing an additional use case in proposed Article 88a (3) GDPR to provide an incentive to use less-intrusive forms of advertising online. Indeed, contextual advertising, which is based on an individual current visit to a single web page or based on a single search query and that involves no retention or link with the individuals past of future activity, is more privacy friendly than behavioural advertising. Although the simple display of contextual advertising does not typically require the use of trackers, such advertising often relies on trackers to measure the performance of advertising campaigns (such as capping cookies, advertising audience measurement cookies, or cookies to combat click fraud). The EDPB and the EDPS consider that such use cases could be considered in the list of cases not requiring consent in Article 88a (3) GDPR. The EDPB and the EDPS therefore invite the co-legislators to consider adding an additional exception in the proposed Article 88a (3) GDPR for contextual advertising, provided that the exception is clearly limited and includes the necessary safeguards to mitigate the risks for the rights and freedoms of individuals[107].

Consent renewal

105. Proposed Article 88a(4) GDPR and proposed Article 37(5) EUDPR provide for additional safeguards when storing or accessing stored personal data in terminal equipment is based on consent, which the EDPB and the EDPS very much welcome. To increase their effectiveness in practice, the EDPB and the EDPS recommend defining a maximum period of validity for consent in the context of proposed Article 88a(4)(b) GDPR and proposed Article 37(5)(b) EUDPR, without prejudice to the right to withdraw consent pursuant to Article 7(3) GDPR. This would ensure that data subjects are reminded at appropriate intervals of their processing choices[108]. Such period could be aligned with the period proposed in Article 88a(4)(c) GDPR or proposed Article 37(5)(c) EUDPR.

106. With regard to proposed Article 88a(4)(c) GDPR and proposed Article 37(5)(c) EUDPR, in order to respect the obligation to not make a new consent request for six months in case of refusal to give consent, controllers will need to record the choice, which may warrant (limited) access to and storage of information in the terminal equipment. The EDPB and the EDPS consider an exception to consent for such scenario should be explicitly added in the Proposal, provided that it would not involve the use of a unique identifier. The recording of the refusal of consent should involve the use of generic information, such as a flag or code, which is common to all data subjects who have refused consent[109].

Oversight and enforcement

107. Proposed Article 88a GDPR and proposed Article 37 EUDPR cannot be implemented and enforced without the provision of supervisory powers. The EDPB and the EDPS therefore point out that it is necessary to provide for supervisory authorities' and the EDPS' fining powers for infringements of proposed Article 88a GDPR and Article 37 EUDPR as amended respectively, by including a reference to the provisions in Article 83(5) GDPR and Article 66(3) EUDPR.

[107] In particular it should be specified that the contextual advertising is based on an individual current visit to a single web page or based on a single search query and that involves no retention or link with the individuals' past of future activity (while still enabling capping cookies limited to the counting of ad displays and is not linked browsing behaviour of individuals).
[108] See also European Commission and EDPB Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation, version for public consultation endorsed on 9 October 2025, para. 164.
[109] EDPB reply to the Commission's Initiative for a voluntary business pledge to simplify the management by consumers of cookies and personalised advertising choices –.DRAFT PRINCIPLES, adopted 13 December 2023, p. 8. See also European Commission and EDPB Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation, version for public consultation endorsed on 9 October 2025, para. 50.

10.2 Automated and machine-readable indications of data subject's choices

108. The EDPB and the EDPS strongly welcome proposed Article 88b GDPR and Article 37(7)-(10) EUDPR that provide for requirements on the use of automated and machine-readable indications of data subjects' choices regarding the processing of their data. They consider that the use of technical means can simplify compliance by controllers, support data subjects in making their online choices, and make such choices effective in practice. This will also help address the issue of cookie fatigue, as data subjects currently have no mechanism to express their preferences across websites and are instead required to repeat them for each visit to a new website.

109. The EDPB and the EDPS understand that the indications concern data subjects' choices with regard to access to and storage of personal data in terminal equipment – and where relevant, subsequent processing of such data – pursuant to proposed Article 88a GDPR and proposed Article 37 EUDPR[110]. They recommend to explicitly specify this link to proposed Article 88a GDPR in proposed Article 88b GDPR and in amended Article 37 EUDPR by making a cross-reference to the relevant provisions.

110. While welcoming this provision, the EDPB and the EDPS would also like to suggest further clarification of the following aspects.

111. With regard to proposed Article 88b(2) GDPR and Article 37(8) EUDPR, the EDPB and the EDPS understand that 'controllers' refers to any controller that accesses or stores data in the terminal equipment of the data subject (e.g. third party cookie providers), not only the controller providing the online interface. The EDPB and the EDPS recommend clarifying this further in the Recitals of the Proposal.

112. The EDPB and the EDPS welcome that, pursuant to proposed Article 88b(4) GDPR, standards will be developed for the interpretation of machine-readable indications of data subjects' choices. Such standards would concern 'the communication of (...) [data subjects'] choices from browsers to websites and from mobile phone applications to web services'[111]. To ensure that the standards achieve their intended effect, and to ensure that all involved actors use the same automated machine-readable indications, the EDPB and the EDPS recommend clarifying who should apply the standards mentioned in proposed Article 88b(4) GDPR. In particular, it should be clarified that the harmonised standards set requirements for all actors involved in the possibility for data subjects to express their choices, pursuant to proposed Article 88b(1) GDPR and proposed Article 37(7) EUDPR. Such actors include controllers under proposed Article 88b(2) GDPR and proposed Article 37(8) EUDPR, and providers of web browsers under proposed Article 88b(6) GDPR.

[110] The EDPB and the EDPS note that Article 88b(1) GDPR refers to the possibility to exercise the right to object pursuant to article 21(3) GDPR through automated and machine-readable means. They note that pursuant to Article 88a GDPR, processing for direct marketing purposes is subject to consent. In case the data subject does not wish their data to be processed for direct marketing purposes, they can refuse or withdraw their consent. It is therefore unclear in what kind of situations the right to object would apply.

[111] Proposal, COM(2025) 836 final, Explanatory Memorandum, p. 7.

113. In line with the principle of data protection by design and default and considering that consent requires a clear affirmative action from the data subject[112], the EDPB and the EDPS recall that the relevant standards should not be configured to consent by default, or that the web browser should prompt the data subject upon first use with a request to make a choice. In addition, to ensure that controllers and providers of web browsers have effective means to comply with their obligations under proposed Articles 88b GDPR and proposed Article 37(7)-(10) EUDPR, the EDPB and the EDPS recommend providing for a timeframe within which the standards would have to be developed and published in the *Official Journal of the European Union*.

114. The Commission has proposed to exclude the providers of web browsers that are SMEs from the scope of proposed Article 88b(6) GDPR. Taking into account the market for web browsers, the EDPB and the EDPS consider such exclusion not to be justified, and therefore recommend not to exclude any providers of web browsers from the scope of proposed Article 88b(6) GDPR.

115. Furthermore, not only web browsers, but also other software used in terminal equipment used by natural persons can play an important role in the communication of data subjects' choices to service providers, e.g. of mobile applications, in particular when such communication is done in conformity with a standard to ensure a harmonised implementation. Therefore, to ensure that the use of automated machine-readable indications would also be effective for other services than websites, the EDPB and the EDPS recommend that proposed Article 88b(6) GDPR would be extended to also apply to providers of other classes of software which may include consumer mobile and desktop operating systems.

116. Pursuant to proposed Article 88b(3) GDPR, proposed Article 88b(1)–(2) GDPR are not applicable to media service providers when providing a media service. In practice, this means that media service providers, when providing a media service, may still decide to request consent, irrespective of the preferences expressed with automated means[113]. The EDPB and the EDPS recommend the co-legislators to reconsider such exception, since it may not contribute to the Proposal's aim to remedy the so-called consent fatigue. Moreover, the processing of personal data for advertising purposes (which often involves e.g. tracking data subjects across services, combining data, and profiling them) when accessing media services is most often not conducted by the media service provider alone. This processing is commonly conducted together with third parties providing components or services that are embedded in the media service's website or mobile app (e.g. to track the data subject or build a profile used for personalised advertisement). Thus, the EDPB and the EDPS recommend treating media service providers in the same way as other service providers.

117. Lastly, similarly to the previous section, the EDPB and the EDPS point out that it is necessary to provide for supervisory authorities' and the EDPS' fining powers for infringements of proposed Article 88b GDPR and Article 37 EUDPR as amended respectively, by including a reference to the provisions in Article 83(5) GDPR and Article 66(3) EUDPR. Additionally, the EDPB and the EDPS also underline the need to ensure effective enforcement with regard to providers of web browsers and, if inclusion in scope were to be supported by the co-legislators based on the above recommendations, also to providers of operating systems[114].

[112] Article 4(11) GDPR and Article 3(15) EUDPR.
[113] See proposed Recital 46.
[114] The GDPR uses the notion of 'controller' or 'processor' For the supervision of proposed Article 88b GDPR, such references may not in all circumstances be adequate as regards the role of providers or web browsers or operating systems. Therefore, some provisions require further amendment to ensure effective enforcement of proposed Article 88b GDPR.

10.3 Repeal of Article 4 ePrivacy Directive

118. Pursuant to Article 5(1) Proposal, Article 4 ePrivacy Directive on security of processing is repealed. The EDPB and the EDPS welcome such deletion to avoid overlap with other legal instruments.

PUBLIC

II. Changes relating to the Data Acquis

11 GENERAL REMARKS

119. The EDPB and the EDPS welcome the objectives of the Proposal to streamline and harmonise rules which form part of the Data Acquis, particularly where it clarifies certain obligations. The EDPB and the EDPS particularly welcome the aim of streamlining the legal framework, where the current Data Acquis has overlaps[115] or is outdated.[116]

120. The aim of this Joint Opinion is not to provide an assessment of all the proposed amendments. Instead, it addresses the most relevant aspects of the Proposal which are of particular importance for the protection of individuals' rights and freedoms, with regard to the processing of personal data.

121. The creation of a single, clearer and horizontal framework is an ambitious aim which, if fulfilled, will help improve legal certainty for businesses and public authorities, maintain the level of protection for data subjects and support the Commission's goal of fostering innovation by enabling trustworthy and responsible access to data. To achieve the full potential of the Commission's ambitions to foster innovation while protecting rights, as set out in the Data Union Strategy[117], trust will be key. The EDPB and the EDPS welcome the support package put forward in the European Data Union Strategy[118] and stand ready to contribute to the Commission's planned guidance on the Data Act[119] where the protection of personal data is concerned.

[115] For example: Regulation (EU) 2018/1807 (Free Flow of Non-Personal Data Regulation) was designed to create a single market for cloud services. It has been partially superseded by Chapter VI of Regulation (EU) 2023/2854 (Data Act) which lays down obligations on switching between data processing services.
[116] For example: Proposed Article 10(3) Data Act would repeal Regulation (EU) 2018/1807 (the Free Flow of Non-personal Data Regulation with the exception of the prohibition of data localisation requirements in the Union.
[117] Communication from the Commission to the European Parliament and the Council: Data Union Strategy Unlocking Data for AI ('Data Union Strategy') dated 19 November 2025, page 2.
[118] Data Union Strategy, page 17.
[119] New guidance on selected definitions of the Data Act, Data Union Strategy, page 17.

12 MAKING DATA AVAILABLE IN CASE OF A PUBLIC EMERGENCY

12.1 Circumstances when personal and non-personal data can be requested

122. The Proposal would amend the rules on the obligation for data holders to make non-personal data available to public sector bodies, the Commission, the European Central Bank ('ECB') and a Union body in case of exceptional need[120]. It defines the types of data which can be requested by bodies that demonstrate an exceptional need to use certain data to carry out their statutory duties in the public interest. What data can be requested, depends on whether data is necessary to respond to a public emergency which the requesting body is unable to obtain 'by other means in a timely and effective manner'[121] or if data is necessary to mitigate or support the recovery from a public emergency[122].

123. By removing the specification under Article 17(2)(e) of the current Data Act (according to which personal data should only be provided in pseudonymised form to requesting bodies, and only when non-personal data is demonstrated to be insufficient to respond to the exceptional need to use the data), the Proposal introduces the possibility for non-pseudonymised personal data to be made available to requesting bodies when responding to a public emergency[123]. The EDPB and the EDPS note that the Proposal does not justify this proposed change or offer any examples of situations in which requests to access non-pseudonymised personal data would be necessary to be able to respond to a public emergency in a timely and effective manner.

124. The EDPB and the EDPS recommend keeping the requirement that the request should concern non-personal data (by default), and only concern personal data in pseudonymised form when non-personal data are not sufficient to respond to the public emergency[124]. Therefore, the EDPB and the EDPS recommend re-inserting Article 17(2)(e) of the current Data Act and deleting the terms 'where possible' from proposed Article 15a(2) Data Act.

125. The EDPB and the EDPS also recommend clarifying the difference between 'responding to [a public emergency]' and 'mitigating or supporting the recovery from [a public emergency]'[125]. This would ensure clarity about the circumstances in which access to personal data in pseudonymised form can be requested by the requesting body, as access to pseudonymised personal data would not be possible in case of 'mitigation or supporting the recovery from a public emergency'.

[120] Chapter V of the current Data Act.
[121] Proposed Article 15a(2) Data Act.
[122] Proposed Article 15a(3) Data Act.
[123] Pursuant to current Article 17(2)(e) Data Act, personal data can only be requested in pseudonymised form. It appears that under the Proposal, which would delete point (e) of Article 17(2) of the Data Act, also non-pseudonymised personal data can be requested by the requesting body. See also proposed Article 15a(2) Data Act which provides that '[w]here the provision of non-personal data is insufficient to address the public emergency, personal data may also be requested and, where possible, made available in pseudonymized form'.
[124] This would also align with Article 18(4) current Data Act, which provides that where the data requested includes personal data, the data holder shall anonymise the data, unless the compliance with the request to make data available to a requesting body requires the disclosure of personal data. In such cases, the data holder shall pseudonymise the data.
[125] Proposed Article 15a(3) Data Act.

12.2 Definition and implementation of technical and organisational measures

126. Article 17(1)(g) Data Act (unaltered by the Proposal) provides that in case of a request of personal data, technical and organisational measures must be specified when making the request. This includes requests for anonymisation or pseudonymisation of the data to be applied by the data holder before making the data available where this is necessary and proportionate to implement data protection principles. Article 19(1)(b) Data Act (unaltered by the Proposal) provides that the requesting body receiving data must have implemented technical and organisational measures to protect personal data and safeguard the rights and freedoms of data subjects. However, the Proposal[126] would remove current Article 17(2)(e) Data Act[127] which requires the requesting body to establish in its request the relevant technical and organisational measures to be taken to protect the pseudonymised personal data.

127. The EDPB and the EDPS recommend ensuring clarity as to who is responsible for defining the relevant technical and organisational measures and who is responsible for implementing them. The EDPB and the EDPS recommend further clarifying the data holder's responsibilities, in particular by specifying that data holders must implement the necessary technical, organisational and legal measures referred to Article 18(1) Data Act, rather than simply 'taking them into account'. This also would correspond with their duty to anonymise or pseudonymise data upon request by public sector bodies concerning personal data pursuant to Article 18(4) Data Act.

12.3 Notification of the request for data by the public sector body to the DPA

128. Article 17(2)(i) Data Act provides that where personal data are requested, public sector bodies must inform the supervisory authority of the Member State in which the public sector body is established, whereas the ECB and Union bodies must inform the Commission of their requests. To promote coherence and to ensure that the EDPS can effectively exercise its responsibilities as responsible authority pursuant to Article 37(3) of the Data Act, the EDPB and the EDPS recommend amending this Article so that it provides that the Commission, the ECB and Union Bodies must also notify the EDPS – as the European counterpart for national supervisory authorities – of their requests for data.

[126] Proposed Article 15a(2) Data Act.
[127] See paragraphs 123 and 124 of this Joint Opinion which recommend reinserting current Article 17(2)(e) Data Act which provides that the request may only concern personal data in pseudonymised form only if it is demonstrated that non-personal data is insufficient to respond to the exceptional need.

13 CHANGES TO THE DATA INTERMEDIATION SERVICES AND ALTRUISM ORGANISATIONS

129. Article 1(18) Proposal aims to modify some of the currently applicable rules on data intermediation services[128] and data altruism organisations[129] and would insert them as a new Chapter VIIa of the Data Act, with the aim of providing a lighter regulatory regime for data intermediaries and data altruism organisations. The EDPB and the EDPS understand and welcome the intention to reduce administrative burden in this domain. However, the objectives of the provisions of the Data Act remain that of increasing trust in data sharing, resulting in more easily accessible and re-usable data[130]. With this in mind, the EDPB and the EDPS put forward a number of targeted recommendations.

13.1 Changes specific to data intermediation services

13.1.1 Voluntary registration of data intermediation services instead of mandatory prior notification

130. Under the Proposal, the registration of data intermediation services providers is voluntary[131], replacing the obligation for all data intermediation services providers to notify the competent authorities prior to the commencement of their services[132]. Without such notification, overall visibility of the services in question towards competent authorities will be reduced, which could hamper effective supervision[133].

131. Transparency and effective oversight foster trust in data intermediation services for data subjects, data users and data sources. Therefore, the EDPB and the EDPS recommend maintaining a prior registration requirement for data intermediation services providers, or at least to maintain this requirement when the intended data intermediation services involve processing of personal data that is likely to result in a high risk to the rights and freedoms of natural persons[134].

[128] Article 2(1) DGA. Proposed Article 38a Data Act.
[129] Article 2(16) DGA. Proposed Article 38a Data Act.
[130] Recital 32 DGA, Commission Staff Working Document, p. 9 and p. 31.
[131] Proposed Article 32e(1), first paragraph Data Act.
[132] Article 11(1) DGA.
[133] Pursuant to the Proposal, data intermediation services may be provided also without registration.
[134] This would correspond with circumstances in which when the processing activities of the data intermediation service provider, taking into account the nature, scope, context and purposes of the processing, are likely to result in a high risk to the rights and freedoms of natural persons. See also Article 35 GDPR.

132. In addition, the Proposal removes certain requirements for recognised data intermediation services providers[135]. The EDPB and the EDPS take note in particular of the removal of the requirements on the format of data, on the procedure for access to the service and on interoperability with other data intermediation services providers[136]. Moreover, some other requirements are retained, but in a modified form[137].

133. In this regard, the EDPB and the EDPS recommend maintaining some of the requirements the Proposal removes. In particular, the EDPB and the EDPS recommend retaining the current provision on the use of tools for obtaining consent from data subjects by recognised data intermediation services providers[138].

134. Also, for the sake of clarity, the EDPB and the EDPS recommend maintaining the following requirements for recognised data intermediation services providers:

i. a requirement to keep a log record of the data intermediation activity, corresponding to with the risks involved[139];

ii. a possibility to use the details collected about activity on the data intermediation service for security and detection of abusive or fraudulent access[140];

iii. a requirement to put procedures in place – corresponding to the risks involved – to prevent fraudulent or abusive practices by service users[141];

iv. a requirement for providers to arrange that, in the event of insolvency, data subjects have an opportunity to exercise their rights[142].

[135] The requirements that would be deleted as effect of the Proposal concern the following points of Article 12 DGA: (d) on format, (f) fair, transparent and non-discriminatory access procedure, (g) preventing fraudulent or abusive access, (h) continuity in case of insolvency, (i) interoperability with other data intermediation services, (k) handling unauthorised transfer, access or use of non-personal data, (l) level of security for non-personal and competitively sensitive information, (n) use of consent/permission tools, (o) a log record of the data intermediation activity. See Explanatory memorandum to the Proposal, 'the list of obligations [requirements for data intermediaries] is drastically shortened', page 17.

[136] Article 12 DGA: (d), (f), (i) DGA.

[137] The requirements of the DGA that would be modified concern the following points of Article 12 DGA: (b) on commercial terms not being dependent on use of other services, (c) on collecting details about usage of the data intermediation service (e.g. the date, time and geolocation data, duration of activity), (e) offering additional tools and services to data holders or data subjects to facilitate the exchange, (j) measures to prevent the transfer of or access to non-personal data that is unlawful under Union or Member State law.

[138] Article 12(n) DGA, which is not maintained in the Proposal, provides that 'where a data intermediation services provider provides tools for obtaining consent from data subjects or permissions to process data made available by data holders, it shall, where relevant, specify the third-country jurisdiction in which the data use is intended to take place and provide data subjects with tools to both give and withdraw consent and data holders with tools to both give and withdraw permissions to process data'.

[139] See Article 12(o) DGA. Insofar as personal data is concerned, the risks for the fundamental rights and freedoms of natural persons should be considered. The DGA also considers other risks, such as risks concerning competitively sensitive information (Article 12(l) DGA).

[140] Proposed Article 32c(b) corresponds with Article 12(c) DGA, except for the removal at the end that use of activity details 'may entail the use of [usage] data for the detection of fraud or cybersecurity'.

[141] See Article 12(g) DGA.

[142] See Article 12(h) DGA.

13.1.2 Functional instead of legal separation of data intermediation services from other services

135. Under the DGA, the data intermediation services provider may not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users and must provide data intermediation services through a separate legal person[143]. The Proposal alters the definition of a 'data intermediation service' and removes the requirement for a separate legal person. Instead, an obligation to keep value-added services functionally separate is introduced, except for micro or small entities[144]. While not opposing the shift to functional separation, the EDPB and the EDPS have certain recommendations to clarify this requirement.

136. To reinforce the purpose limitation rule in the proposed Article 32c(a) Data Act, neutrality of data intermediation should be ensured[145]. For this reason, the EDPB and the EDPS recommend including clear criteria for functional separation. The fulfilment of such criteria should be verifiable for the supervisory/competent authority and might include requirements to have technical and organisational segregation of data as well as separate management, financing and staff.

137. Further, such functional separation within the same legal person should be required on the one hand between the provision of the data intermediation service, and on the other hand all other activities of the data intermediation services provider (not only with regard to value-added services). Such an adjustment serves the interest of neutrality, as well as legal certainty, given the lack of criteria or definition to determine which other activities are value-added services.

138. Last, the Proposal does not specifically justify the reason for exempting small and micro enterprises entirely from the functional separation requirement[146]. Ensuring neutrality by managing conflicting interests would appear relevant, regardless of enterprise size.

13.2 Changes specific to data altruism organisations

139. The Proposal removes record-keeping and reporting obligations for recognised data altruism organisations[147].

140. To foster trust in the label 'data altruism organisation recognised in the Union'[148], effective public oversight should be ensured and appropriate accountability mechanisms should be put in place. For this reason, the EDPB and the EDPS recommend maintaining the record-keeping obligation, in order to ensure that competent authorities can exercise their oversight in an effective manner.

[143] Article 12(a) DGA.
[144] Proposed Article 32c(d)(iii) Data Act. Proposed Article 32c(a) Data Act maintains the requirement that providers 'do not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users.
[145] See Recital 33 of the DGA.
[146] Proposed Article 32c(d)(iii) Data Act
[147] Article 20 DGA is repealed by the Proposal.
[148] Article 17(2) DGA and corresponding proposed Article 32a(3)(b) Data Act.

141. The EDPB and the EDPS also recommend maintaining certain elements of the reporting obligation for recognised data altruism organisations, in order to foster effective oversight. In particular, an annual overview of the categories of all natural and legal persons that were allowed to process data could be required. Also, an overview of the sources of revenue of the recognised data altruism organisation, in particular all revenue from allowing access to the data, and on categories of expenditures[149] could be required on an annual basis.

142. Harmonisation across the EU, for example through an implementing act, could be considered to determine common elements for all annual reports.

143. The EDPB and the EDPS recommend maintaining the requirement to keep track of the objectives of general interest pursued by anyone using the data held by the recognised data altruism organisation[150] as part of the record-keeping obligation, rather than as part of an annual report. The same applies for the description of the technical means used, including of the techniques used to preserve privacy and data protection[151].

13.3 Application forms for registering data intermediation service providers and data altruism organisations

144. The Proposal no longer harmonises the information to be provided for the voluntary registration as data intermediation services provider[152] or as data altruism organisation throughout the EU. Instead, the Proposal provides that 'competent authorities shall establish the necessary application forms'[153]. At the same time, registration in one Member State leads to inclusion in the public Union register and is valid in all Member States[154].

145. Given the role that registration plays in enabling competent authorities to exercise oversight over recognised data intermediation services providers and data altruism organisations, the lack of harmonisation of the application forms throughout the EU will likely lead to fragmentation.

146. The EDPB and the EDPS recommend harmonising the application form across the EU, for instance through an implementing act, to ensure consistency. Such an implementing act could set out the required description of the intended nature of data intermediation or data altruism processing activities, such as types of data, including categories of personal data and intended value-added services. The application form should ensure that competent authorities receive sufficient and reliable information to be aware of and enable supervision of the data intermediation and data altruism activities being pursued.

[149] Article 20(2)(e) DGA. Where the current provisions mention 'expenditure', the EDPB and the EDPS understand this to mean a high-level overview of expenditures.
[150] Article 20(2)(c) DGA.
[151] Article 20(2)(c) DGA.
[152] Article 11(6) and 19(4) DGA. Article 11 DGA imposed a prior notification obligation upon data intermediation services providers and listed the information to be provided in paragraph 6.
[153] Proposed Article 32e(3) Data Act.
[154] Proposed Article 32e(4) Data Act.

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

147. The proposed Article 32g Data Act significantly modifies the current provisions in Articles 14 and 24 DGA. The existing DGA allows competent authorities to monitor and supervise data intermediation servicesproviders or data altruism organisations if a natural or legal person requests it. In contrast, the proposed Article 32g(1) Data Act mandates competent authorities to initiate supervision upon their own initiative or on a request by a natural or legal person. This amendment seems to introduce a change from discretionary power to mandatory action. If this is the case, the EDPB and the EDPS recommend amending this provision to maintain the competent authorities' discretion to prioritise enforcement action. By maintaining this discretion, competent authorities will be in a better position to allocate resources more efficiently to take action where it is most needed.

148. The EDPB and the EDPS have not identified an explanation for the modification in the Explanatory Memorandum or in the Recitals and recommend keeping the current wording ('... may monitor … on basis of a request…').

14 RE-USE OF DATA AND DOCUMENTS HELD BY PUBLIC SECTOR BODIES

149. The EDPB and the EDPS welcome the objective of the Proposal to simplify the regulatory framework for the use of data and documents held by public sector bodies. To achieve this aim, the Commission has proposed integrating the provisions of the ODD and certain provisions of the DGA[155] under a single regulation, namely the Data Act. In doing so, the Proposal aims to address the lack of clarity and consistency between the existing rules of the DGA and of the ODD (as implemented under Member States' laws) concerning the re-use of documents held by public sector bodies[156].

150. The Proposal combines the rules of Chapter II of the DGA and of the ODD under a new Chapter VIIc of the Data Act[157]:

   i. Section 1 of this new Chapter sets out the general provisions applicable to all cases referred to in this Chapter, notably provisions on non-discrimination (of possible re-users)[158], on exclusive arrangements[159] and on general principles relating to charging[160].

   ii. Section 2, on re-use of open government data, contains provisions related to data and documents re-usable for commercial or non-commercial purposes[161], as well as on specific categories of data which are 'open by default', such as research data[162] and high-value datasets[163], which are subject to specific rules[164].

[155] Articles 5-9 of the DGA would be inserted, with modifications, into Section 3 of Chapter VIIc of the Data Act.
[156] See Recitals 21-24 Proposal.
[157] See Recital 22 Proposal. See also Explanatory Memorandum, p. 17-19.
[158] Proposed Article 32j Data Act.
[159] Proposed Article 32k Data Act.
[160] Proposed Article 32l Data Act.
[161] Proposed Articles 32n-32s Data Act.
[162] Proposed Article 32t Data Act.
[163] Proposed Article 32u Data Act.
[164] Proposed Article 32v Data Act.

iii. Section 3 of the new Chapter, on the re-use of certain categories of protected data, contains provisions of the repealed DGA[165] and applies to public sector bodies making available for re-use certain categories of protected data[166].

151. As a general comment, applicable to all provisions of the new Chapter VIIc of the Data Act, the EDPB and the EDPS note that Article 1(2) DGA, which provides that the DGA 'does not create any obligation on public sector bodies to allow the re-use of data, nor does it release public sector bodies from their confidentiality obligations under Union or national law', is not retained in the Proposal. The specification under the current rules that there is no legal duty for public sector bodies to give access to personal data is important from a data protection viewpoint. For this reason, the EDPB and the EDPS recommend reinstating Article 1(2) DGA[167].

152. The EDPB and the EDPS also note the Proposal would delete the provisions in Article 1(3) DGA, which clarify that 'the Regulation does not create a legal basis for the processing of personal data, nor does it affect any of the rights and obligation set out in Regulations (EU) 2016/679'. For clarity, the EDPB and the EDPS recommend inserting an equivalent provision in the Proposal in relation to access granted by public bodies for re-use, governed by proposed Chapter VIIc, and in relation to activities of data intermediation services and data altruism organisations, governed by Chapter VIIa.

153. In addition, the EDPB and the EDPS recommend to further clarify the relationship between the different access regimes in sections 2 and 3 of new Chapter VIIc of the Data Act,[168] in order to achieve the objective of providing greater legal clarity to public sector bodies and potential re-users, while not lowering the level of protection of personal data. Otherwise, the relationship between the access regimes under the Data Act and national rules[169], which govern the re-use of personal data in this context[170], continues to be complex and unclear.

154. The Proposal lists requirements that public sector bodies can establish to preserve the protected nature of data and documents to which they grant access for re-use, without the use of a secure processing environment. Two of the proposed requirements are the same as those set out in the DGA, namely anonymisation (for personal data) and disclosure control (for commercially confidential information or intellectual property). The Proposal adds a third possibility, namely granting access subject to other 'forms of preparation of personal data'[171]. The EDPB and the EDPS understand that this means that access could be granted to personal data for re-use without anonymising this data. The EDPB and the EDPS have not identified an explanation for including this new possibility in neither the Explanatory Memorandum nor the Recitals. They consider that the necessity should be analysed and duly justified in the Recitals, keeping in mind the principle of data minimisation. In case the co-legislators deem this modification justified, the EDPB and the EDPS recommend that the co-legislators clarify what technical measures, other than pseudonymisation, are covered by these 'preparations' or at least to set out their objectives.

---

[165] Articles 5-9 of the DGA.
[166] Proposed Articles 32w-32ab Data Act.
[167] For instance, in Article 32i Data Act.
[168] One cause of complexity is the definition of 'certain categories of protected data' (proposed Article 2(54) Data Act), which is dependent on whether personal data falls outside the scope of Section 2 of Chapter VIIc. In turn, the scope of Section 2 of Chapter VIIc is dependent on the scope of national access regimes (proposed Article 32i(3)(b)(ii) Data Act). Understanding the scope of Section 3 of Chapter VIIc requires reading (at least) proposed Articles 32i(4)(a) and 2(54) Data Act together, containing three negations: 'Section 3 of this Chapter does *not* apply to (a) data and documents that are *not* certain categories of protected data', meaning data 'protected on the grounds of ... (d) the protection of personal data, insofar as such data fall *outside* the scope of Section 2 of Chapter VIIc' (emhpasis added).
[169] Proposed Article 32i(5) Data Act. See also proposed Article 1(13) Data Act: 'With regards to data and documents in scope of Section II of Chapter VIIc, Chapter VIIc of this Regulation 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.'
[170] Proposed Article 32i(9) Data Act, cross-referencing to Article 2(54), including at letter (d) 'the protection of personal data'.
[171] Proposed Article 32w(3)(a)(ii) Data Act.

155. In relation to the proposed Section 3 Chapter VIIc Data Act concerning the re-use of protected data and documents including when they contain personal data, the EDPB and the EDPS note that the provision in Article 32w(5)(a)[172] seems superfluous in light of Article 1(5) Data Act and proposed 32w(2)(c) Data Act. Against this background and bearing in mind that this provision could cause confusion, the EDPB and the EDPS recommend the co-legislators to delete this provision.

15 ENFORCEMENT BY AND COOPERATION BETWEEN COMPETENT AUTHORITIES AND OTHER AUTHORITIES

15.1 Horizontal application of the implementation and enforcement provisions of the proposed Data Act

156. As the Proposal merges the Data Acquis into the Data Act, Chapter IX of the Data Act on implementation and enforcement applies horizontally to all Chapters of the Data Act pursuant to the Proposal, including the Chapters on access to data in case of public emergency[173], re-use of data and documents held by public sector bodies[174], and data intermediaries and data altruism organisations[175].

15.1.1 Designation of competent authorities to oversee Proposed Chapter V Data Act and relationship with horizontal oversight provisions in Proposed Chapter IX Data Act

157. Article 37(1) Data Act requires Member States to have designated one or more competent authorities to be responsible for the application and enforcement of the Data Act. In the view of the EDPB and the EDPS, this provision would also cover the designation of competent authorities for the new Chapters. Yet the requirement to designate competent authorities, in accordance with Article 37(1) of the current Data Act, is also separately included in Chapter VIIa[176] and in Chapter VIIc[177]. The specific provisions defining the tasks of the competent authorities are also included in these Chapters[178], rather than in the overarching Chapter IX on enforcement. To ensure legal certainty, the EDPB and the EDPS recommend clarifying the relationship between the relevant provisions of Chapters VIIa and VIIc and Chapter IX.

[172] Article 32w(5)(a): 'where there is no (GDPR) legal basis other than consent for transmitting the data, the re-use of data and documents shall only be possible with the consent of the data subject'.
[173] Chapter V Data Act.
[174] New Chapter VIIc Data Act.
[175] New Chapter VIIa Data Act.
[176] Proposed Article 32b Data Act.
[177] Proposed Article 32z Data Act.
[178] Proposed Articles 32b, 32g, 32z Data Act.

15.1.2 Right to lodge a complaint regarding Proposed Chapter V and relationship with horizontal complaint provisions in Chapter IX Proposed Data Act

158. The Proposal inserts an Article 22a in Chapter V on the right to lodge a complaint, regrouping the rights to complain previously spread over Articles17(5), 18(5), 20(5) and 21(5), with the competent authority of the Member State where the data holder is established specifically for disputes concerning requests for data in a public emergency under proposed Article 15a Data Act. The inclusion of this provision outside of the horizontal Chapter IX Data Act raises questions on the applicability of proposed Article 38(2)–(3) Data Act. The EDPB and the EDPS recommend clarifying the relationship between proposed Article 22a and proposed Article 38 Data Act, or merging proposed Article 22a and proposed Article 38 Data Act to ensure legal certainty.

15.1.3 Specific redress mechanism for the re-use of public sector data in Proposed Chapter VIIc and relationship with horizontal redress provisions in Proposed Chapter IX Data Act

159. The EDPB and the EDPS note that Chapter VIIc on the re-use of public sector data maintains the provisions on redress from the Open Data Directive[179] and the DGA[180]. The EDPB and the EDPS recommend clarifying how proposed Articles 32m, 32o(4) and 32ab(2) Data Act relate to proposed Article 38 and current Article 39 Data Act.

15.2 Cooperation and information exchange between competent authorities and other relevant authorities

160. The current Data Act provides that Member States must ensure the cooperation of competent authorities and, where relevant, with the Commission or the EDIB, 'to ensure the consistent and efficient application of this Regulation, including the exchange of all relevant information by electronic means, without undue delay'[181]. Member States shall also provide the necessary powers for cooperation among relevant competent authorities responsible for other Union or national legal acts, including the GDPR, to ensure the Data Act is 'enforced consistently with other Union and national law'[182].

161. However, the EDPB and the EDPS note that the Proposal would remove Article 38(3) current Data Act which governs competent authorities' cooperation to 'handle and resolve complaints effectively and in a timely manner, including by exchanging all relevant information by electronic means, without undue delay'. The EDPB and the EDPS would recommend re-inserting Article 38(3) current Data Act to allow cooperation, including the exchange of information, between competent authorities when handling complaints. This will provide more legal certainty for how cooperation should function and reduce the risk of possible future legal disputes on procedural matters.

[179] Proposed Article 32m and 32o(4), corresponding with Article 4(4) Open Data Directive.
[180] Proposed Article 32ab(3), corresponding with Article 9(2) DGA.
[181] Article 37(5)(f) current Data Act.
[182] Article 37(5)(g) current Data Act.

162. The EDPB and the EDPS consider it important to also enable the efficient exchange of relevant information for cooperation between competent authorities under the Data Act and competent authorities responsible for other Union or national legal acts, such as the GDPR. The exchange of information should cover all enforcement matters, including the handling of complaints and procedures initiated by the authorities themselves[183]. The Data Act presently does not provide for an explicit legal basis for the exchange of relevant information across regulatory domains. The EDPB and the EDPS recommend providing an explicit legal basis for the exchange of all relevant information, including information obtained in the context of enforcement activities[184]. This would enable the effective and consistent enforcement of the Data Act and other Union or national legal acts, but also to provide legal certainty for the enforcers and limit possible legal disputes on procedural matters.

15.3 Clarification of Articles 37(3) and 40(4) Data Act

163. Articles 37(3) and 40(4) of the current Data Act refer to responsibilities and competences for supervisory authorities under the GDPR in relation to the processing of personal data with regard to the monitoring and enforcement of the Data Act. The EDPB and the EDPS welcome the Data Act's explicit recognition of the competences of supervisory authorities under the GDPR. However, the EDPB and the EDPS are concerned that the allocation of responsibilities between competent authorities under Article 37(1) Data Act and supervisory authorities, related to the monitoring of the application of the Data Act insofar as the processing of personal data is concerned, is ambiguous and consider that further clarification is warranted[185].

164. The EDPB and the EDPS consider that the Data Act should clearly indicate that data protection supervisory authorities participate in the monitoring of the application of the Data Act on the basis of their existing competences and responsibilities under the GDPR only. At the same time, it remains of utmost importance to ensure that the designated competent authority under Article 37(1) Data Act has a clear duty to cooperate with the supervisory authority under the GDPR whenever relevant, in order to ensure a consistent application of the GDPR and the Data Act[186]. Therefore, it should be clarified that, as part of such cooperation, the supervisory authority under the GDPR must be consulted by the authority designated under Article 37(1) Data Act to provide their assessment in cases that require an assessment of EU and national data protection law. Such cases might, for example, concern whether a data holder correctly qualifies which data should be considered personal data or whether a valid legal basis under the GDPR exists for a user who is not a data subject[187].

[183] Which is more specific than Article 37(5)(f) current Data Act which governs the cooperation of competent authorities.
[184] To this end, inspiration could be drawn from Article 13(3) of the DGA (not maintained under the Proposal), which provides: 'The powers of the competent authorities [...] are without prejudice to the powers of the data protection authorities, national competition authorities, authorities in charge of cybersecurity and other relevant sectoral authorities. In accordance with their respective competences under Union and national law, those authorities shall establish strong cooperation and exchange information as is necessary for the exercise of their tasks [...],and shall aim to achieve consistency in the decisions taken in applying this Regulation.' For the sake of clarity, the possibility for competent authorities and supervisory authorities to exchange information relating to ongoing investigations should be addressed explicitly.
[185] In relation to the initial Commission Proposal for the Data Act see also EDPB-EDPS Joint Opinion on Data Act, paras. 99-103.
[186] Articles 37(5)(g) of the current Data Act.
[187] See also the additional examples given in Question 2 of the Commission Frequently Asked Questions Data Act, 12 September 2025, version 1.3.

165. The EDPB and the EDPS recommend the co-legislators to use the opportunity of simplifying the Data Acquis to clarify the roles and responsibilities of supervisory authorities under the GDPR and their envisaged cooperation with competent authorities under the Data Act. The clarification of the current Articles 37(3) and 40(4) Data Act is important to ensure legal certainty regarding the respective competences of the authorities designated as competent authorities under the Data Act and the supervisory authorities under GDPR. Clarification is also important to ensure effective oversight and enforcement[188].

16 EDIB: CHANGES TO STRUCTURE AND ROLE

166. The DGA provides that the Commission must establish a European Data Innovation Board ('EDIB') in the form of an expert group[189] and it sets out the EDIB's tasks[190]. The current Data Act entrusts additional tasks to the EDIB[191].

167. In terms of membership and structure, the EDPB and the EDPS support the increased flexibility introduced by the Proposal[192], which should allow the EDIB to adapt to future developments and priorities.

168. The EDPB and the EDPS welcome the Proposal's confirmation of the EDIB's role in supporting the consistent application of the Data Act, in particular by 'serving as a forum for strategic discussions on data policies, data governance, international data flows and cross-sectoral developments relevant to the European data economy'[193]. With the proposed changes, the EDIB should be in a better position to also discuss common strategic issues that arise across different EU regulations.

169. The Proposal sets out the role of the EDIB in a more concise manner than the DGA and current Data Act. In this regard, the EDPB and the EDPS recommend that the EDIB's role in 'facilitating cooperation between competent authorities through capacity-building and the exchange of information'[194] should remain the same as under the current Data Act. Therefore, the EDPB and the EDPS recommends to reinsert the phrase 'in particular by establishing methods for the efficient exchange of information relating to the enforcement of the rights and obligations (...) in cross-border cases, including coordination with regard to the setting of penalties'[195].

170. Moreover, the EDPB and the EDPS note that the Data Act empowers the Commission with issuing guidelines with the advice of EDIB with respect to certain provisions (e.g. Article 9(5), 32(3) and 33(1)). In this regard, the EDPB and the EDPS recommend clarifying that one of the tasks of the EDIB is to advise and assist the Commission with the development of guidelines and standards[196].

[188] In relation to the initial Commission Proposal for the Data Act see also the EDPB-EDPS Joint Opinion on Data Act, paras. 99-103.
[189] Article 29(1) DGA.
[190] Article 30 DGA.
[191] Article 42 of the current Data Act.
[192] Article 1(22) Proposal, inserting Article 41a 'European Data Innovation Board' in the Data Act, gives the Commission the power to 'decide to add additional categories of members' and 'decide on the composition of the different configurations in which the Board will fulfil its tasks'.
[193] Proposed Article 1(23).
[194] Proposed Article 1(23), replacing Article 42 Data Act.
[195] Article 42(b) current Data Act.

171. The EDPB and the EDPS also recommend empowering the Commission to issue guidelines on any topic concerning the Data Act, in order to facilitate its effective application and enforcement. Where appropriate, such guidance should be drafted in close cooperation with relevant sectoral authorities or bodies.

172. If the recommendations above are followed by the co-legislators, it should enable the Commission to develop joint guidelines with e.g. the EDPB as a sectoral body, where the protection of personal data is concerned also in light of Article 8(3) of the Charter and in line with Article 1(5) of the Data Act. These changes would also allow the EDIB to advise and assist the Commission on the development of any guidelines in line with the recommendation in paragraph 170 of this Opinion.

PUBLIC