EDPB-EDPS Joint Opinion 02/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)

Adopted on 4 May 2022

Executive summary

With this Joint Opinion, the EDPB and the EDPS aim to draw attention to a number of overarching concerns on the Proposal on Data Act and urge the co-legislature to take decisive action.

The EDPB and EDPS note that the Proposal would apply to a broad range of products and services, including the connected objects ('Internet of Things'), medical or health devices and virtual assistants. Certain products and services may even process special categories of personal data, such as data concerning health or biometric data. As the Proposal does not explicitly exclude certain types of data of data from its scope, data revealing highly sensitive information about individuals could become the object of data sharing and use according to the rules established in the Proposal.

While welcoming the efforts made to ensure that the Proposal does not affect the current data protection framework, the EDPB and the EDPS consider that additional safeguards are necessary to avoid lowering the protection of the fundamental rights to privacy and to the protection of personal data in practice. First, additional safeguards are especially necessary as the rights to access, use and share data under the Proposal would likely extend to entities other than the data subjects, including businesses, depending on the legal title under which the device is being used. Second, the EDPB and EDPS are deeply concerned by the provisions of the Proposal regarding the obligation to make data available to public sector bodies and Union institutions, agencies or bodies in case of "exceptional need". Finally, the EDPB and the EDPS are concerned that the oversight mechanism established by the Proposal may lead to fragmented and incoherent supervision.

1. The rights to access, use and share data

To limit the risks of an interpretation or implementation of the Proposal that could affect or undermine the application of existing data protection law, the EDPB and the EDPS call on the co-legislator to explicitly specify that data protection law "prevails" in case of conflict with the provisions of the Proposal insofar as the processing of personal data is concerned.

In order to promote data minimisation, products should be designed in such a way that data subjects are offered the possibility to use devices anonymously or in the least privacy intrusive way as possible, irrespective of their legal title on the device. Data holders should also limit as much as possible the amount of data leaving the device (e.g. by anonymising data).

Furthermore, the enhancement of the right to data portability mentioned in Recital 31 as one of the goals of the Proposal would require, in so far as personal data are involved, an effective empowerment of data subjects so to give them more control over their personal data. As the definition of 'user' encompasses legal persons, in case of exercise of this right by a business, this takes the form of a commercial obligation for the manufacturer/data holder to provide access to data to businesses and allow its exploitation, rather than the individuals' 'right' to access and port their personal data. In fact, according to the concept of 'user' adopted by the Proposal, individuals become entitled to enhanced portability right only incidentally, depending on the legal title under which they use the product or the related service (ownership, rental or lease) rather than on their relationship with the information concerning their private use of the product or service.

Therefore, to achieve an effective empowerment of individuals with regard to their personal data, the concept of user in Article 2(5) of the Proposal and throughout the text needs to be integrated and specified as follows: (a) adding in the definition of users ''and the data subjects'' (b) clearly differentiating the situations where the user is the data subject from the situation where the user is not the data subject.

Moreover, the EDPB and the EDPS recommend specifying that where the user is not the data subject, any personal data generated by the use of a product or related service shall only be made available to the user in compliance with in particular Article 6 and 9 GDPR and on the condition that, were relevant, the requirements of Article 5(3) ePrivacy Directive are fulfilled. Similar considerations apply to the making available of data to third parties upon request of a business user.

The EDPB and the EDPS stress the need to ensure that access, use, and sharing of personal data by users other than data subjects, as well as by third parties and data holders, should occur in full compliance with all of the provisions of the GDPR, EUDPR and ePrivacy Directive, including informing data subjects about the access by controllers to their personal data and facilitating the exercise of data subject rights by controllers. The EDPB and the EDPS also recall that it is important to ensure that any further processing of personal data complies in particular with Article 6(4) GDPR and, having specific regard to the possibility of automated decision-making, including profiling, with the relevant obligations provided under Article 22 GDPR.

The EDPB and the EDPS also recommend to include in the proposal clear limitations or restrictions on the use of personal data generated by the use of a product or service by any entity other than data subjects, in particular where the data at issue are likely to allow precise conclusions to be drawn concerning their private lives or would otherwise entail high risks for the rights and freedoms of the individuals concerned. In particular, the EDPS and EDPB recommend to introduce clear limitations regarding use of personal data generated by the use of a product or related services for purposes of direct marketing or advertising, employee monitoring, credit scoring or to determine eligibility to health insurance, to calculate or modify insurance premiums. This recommendation is without prejudice to any further limitations that may be appropriate, for example to protect vulnerable persons, in particular minors, or due to the particularly sensitive nature of certain categories of data (e.g. data concerning the use of a medical device or biometric data) and the protections offered by Union legislation on data protection.

2. The obligation to make data available in case of “exceptional need”

As regards Chapter V of the Proposal, the EDPB and the EDPS have deep concerns on the lawfulness, necessity and proportionality of the obligation to make data available to public sector bodies and Union institutions, agencies or bodies in case of “exceptional need”.

The EDPB and the EDPS recall that any limitation on the right to personal data must be based on a legal basis that is adequately accessible and foreseeable and formulated with sufficient precision to enable individuals to understand its scope. In accordance with the principles of necessity and proportionality, the legal basis must also define the scope and manner of the exercise of their powers by the competent authorities and be accompanied by sufficient safeguards to protect individuals against arbitrary interference.

The EDPB and the EDPS observe that the circumstances justifying the access are not narrowly specified and consider it necessary for the legislator to define much more stringently the hypotheses of emergency or exceptional need. Moreover, the EDPB and the EDPS consider certain public sector bodies and Union institutions, agencies and bodies should be excluded from the scope of Chapter V as such and should only be able to oblige data holders to make data available in accordance with the powers provided by sectoral legislation.

3. Implementation and enforcement

The EDPB and the EDPS highlight the risk of operational difficulties that might result from the designation of more than one competent authority responsible for the application and enforcement of the Proposal. The EDPB and the EDPS have serious concerns that this governance architecture will lead to complexity and confusion for both

organisations and data subjects, to divergence in regulatory approaches across the Union and thus affect consistency of monitoring and enforcement.

The EDPB and the EDPS welcome the designation of the data protection supervisory authorities as competent authorities responsible for monitoring the application of the Proposal insofar as the protection of personal data is concerned, which is important to avoid inconsistencies and possible conflicts between the provisions of the Proposal and data protection laws, and to preserve the fundamental right to the protection of personal data as established under Article 16 of the Treaty on the Functioning of the European Union (TFEU) and Article 8 of the Charter of fundamental rights of the European Union.

The EDPB and the EDPS ask the co-legislators to also designate national data protection supervisory authorities as coordinating competent authorities under this Proposal. Data protection supervisory authorities have a unique expertise, both legal and technical, in the monitoring of the compliance of data processing. Moreover, the EDPB and the EDPS are of the opinion that, considering that the GDPR applies when personal and non-personal data in a data set are inextricably linked, the role of data protection authorities should prevail in the governance architecture of the Proposal.

Having regard the oversight role of the EDPS as the data protection authority for the European Union institutions, bodies and agencies and the fact that some of the European Union institutions, bodies and agencies may also act as user or a data holder within the meaning of this Proposal, the EDPB and the EDPS recommend including a reference to the EDPS as competent authority for the supervision of the whole Proposal insofar as it concerns the Union institutions, bodies, offices and agencies.

Table of Contents

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,

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

HAVE ADOPTED THE FOLLOWING JOINT OPINION

1 BACKGROUND

1. The Proposal on Data Act ("the Proposal") is enacted pursuant to the Communication "A European Data strategy for data ("the Data Strategy")[1].

2. The European Data Protection Board ("EDPB") and the European Data Protection Supervisor ("EDPS") notice that, according to the Commission"*citizens will trust and embrace data-driven innovation only if they are confident that any personal data sharing in the EU will be subject to full compliance with the EU's strict data protection rules*"[2].

3. As specified in its Explanatory Memorandum, the Proposal "*is a key pillar and the second major initiative announced in the Data Strategy. In particular, it contributes to the creation of a cross-sectoral governance framework for data access and use by legislating on matters that affect relations between data economy actors, in order to provide incentives for horizontal data sharing across sectors"*. The specific objectives of the Proposal are the following:

- *"Facilitate access to and the use of data by consumers and businesses, while preventing incentives to invest in ways of generating value through data.*

- *Provide for the use by public sector bodies and Union institutions, agencies or bodies of data held by enterprises in certain situations where there is an exceptional data need.*

- *Facilitate switching between cloud and edges services.*

- *Put in place safeguards against unlawful data transfer without notification by cloud service providers.*

- *Provide for the development of the interoperability standards for data to be reused between sectors"*[3].

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions "A European strategy for data", 19 of February 2020, COM (2020) 66 final.
[2] A European strategy for data, Introduction, page 1.
[3] Explanatory Memorandum, page 3.

2 SCOPE OF THE OPINION

4. On 23 February 2022, the Commission published the Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data ("Data Act") or ("the Proposal").

5. On 23 February 2022, the Commission requested a Joint Opinion of the EDPB and the EDPS ("Opinion") on the basis of Article 42(2) of Regulation (EU) 2018/1725 (EUDPR) on the Proposal.

6. **The Proposal is of particular importance for the protection of individuals' fundamental rights and freedoms with regard to the processing of their personal data. The scope of the Opinion is limited to the aspects of the Proposal related to and involving personal data, which constitute one of the main pillars of the Proposal.**

7. The EDPB and the EDPS welcome Recital 7 of the Proposal, where it is explicitly mentioned that the Proposal complements and is without prejudice to Union law on data protection and privacy, in particular GDPR and e-Privacy Directive.

8. The EDPB and the EDPS highlight that **it is necessary to ensure and uphold the respect and the application of the EU acquis in the field of personal data protection. When personal data are involved in the context of the Proposal, it is essential to clearly avoid in the legal text of the Proposal any inconsistency and possible conflict with the GDPR, e-Privacy Directive or EUDPR**. This not only for the sake of legal certainty, but also to avoid that the Proposal has the effect of directly or indirectly jeopardizing the fundamental rights to privacy and the protection of personal data, as established under Articles 7 and 8 of the Charter of fundamental rights of the European Union (the "Charter") and Article 16 of the Treaty on the Functioning of the European Union (''TFEU'').

9. Since the Proposal, as further explained in this Opinion, raises several concerns regarding the protection of the fundamental rights to privacy and the protection of personal data, **the aim of this Opinion is not to provide an exhaustive list of all the issues, nor always to provide alternative proposals of wording suggestions**. Instead, **this Opinion aims at addressing the main criticalities, with respect to privacy and data protection, of the Proposal**.

3 ASSESSMENT

3.1 General comments

10. The EDPB and the EDPS acknowledge the goal to unleash the potential of information to be extracted from data in order to gain valuable knowledge for important common values and for health, science, research and climate action. In addition, they highlight that the GDPR already allows for this as far as personal data are concerned.

11. The EDPB and the EDPS also acknowledge the importance of and welcomes the aim of providing a more effective right to data portability, with a view of facilitating innovation and promoting competition and to empower consumers using products or related services to meaningfully control how the data generated by their use of the product or related service are used[4].

[4] Explanatory Memorandum, p. 13.

12. The Proposal aims to lay down harmonised rules on making data generated by the use of a product or related service available to the user of that product or service and on the making data available by data holders to data recipients[5]. The EDPB and EDPS therefore recognise that the envisaged scope of application of the Proposal does not exclusively concern personal data, but instead would apply to both personal and non-personal data that are generated by the use of products are services within the meaning of the Proposal.

13. The EDPB and the EDPS note, however, that the enhanced right to portability would extend to **a broad range of products and services that may reveal highly sensitive data** concerning individuals, including children and other vulnerable categories of data subjects. The Proposal explicitly targets data generated by the IoT and IoB, including vehicles, home equipment and consumer goods, medical and health devices.[6] The data generated by these connected objects will become subject matter of the data access rights and obligations introduced by the Proposal. As a result, data from the most private places and surroundings of data subject may be processed, as well as highly sensitive health data.

14. The Proposal does not distinguish between personal data, as defined under Article 4(1) of the GDPR, and other non-personal data in defining the scope of the rights of access, sharing and use of data. Moreover, **the rights to access, use and share data under the Proposal would in practice likely extend to entities other than the data subject**, including businesses, depending on the legal title under which the product is used. The data sharing rights and obligations that the Proposal intends to set up therefore create a **substantial risk of personal data being collected, shared and used without knowledge of the data subject**, notably if not specified according to the recommendations made in this Opinion, in particular in case of exercise of the right to data portability by a user other than the data subject. Illustrations of problematic use cases include, without being limited to, devices tracking the location of products or services carried or operated by data subjects which are not "users" in the sense of the Proposal.

15. The EDPB and the EDPS are concerned that the Proposal in its current text would extensively push a development towards "commodification" of personal data, whereby personal data are seen as a mere tradeable commodity. This would not only undermine the very concept of human dignity and the human-centric approach the EU wants to uphold in its Data Strategy, but it would also risk undermining the rights to privacy and data protection as fundamental rights[7].

16. The EDPB and the EDPS acknowledge and welcome the efforts made to ensure that the Proposal does not affect the current data protection regime provided by the GDPR and the ePrivacy Directive. That being said, the EDPB and the EDPS consider that **additional safeguards are necessary** to avoid lowering the protection of the fundamental rights to privacy and to the protection of personal data in practice.

17. In the remainder of this Opinion, the EDPB and the EDPS provide recommendations on how to make the relevant data protection principles, safeguards and obligations more effective within the Proposal. Given the wide scope of the rights and obligations set out in the Proposal with regard to data access, use and sharing, general references to the GDPR are not sufficient. The EDPB and the EDPS consider further specifications necessary, in particular where the text of the Proposal risks giving rise to misinterpretation if a more complete reference to data protection law (both GDPR and ePrivacy

[5] Article 1(1) of the Proposal.
[6] Recital (14) of the Proposal.
[7] See in this regard also https://edpb.europa.eu/system/files/2021-05/edpb_statementondga_19052021_en_0.pdf p. 4.

Directive) is not explicitly highlighted. The EDPB and the EDPS consider that, absent such specifications, there is a risk that the Proposal lowers the level of protection for data subjects, contrary to the stated objectives of Commission.

18. These recommendations are also due to the unclear scope (referring to non-personal and/or to personal data) of the rights and obligations to access to, share and use data by data holders, users (as non-data subjects) and third parties or recipients laid down in the Proposal.

19. Therefore, the EDPB and the EDPS remark that, considering that the enhanced right to portability would extend to a broad range of products and services that may reveal highly sensitive data concerning individuals, in order not to undermine the level of protection of personal data, the Proposal should expressly and clearly specify that processing of personal data by data holders, users (as non-data subjects) and third parties or recipients shall be subject to all conditions and rules provided by data protection legislation[8].

3.2 Interplay of the Proposal with EU data protection laws

20. The EDPB and the EDPS note that Article 1(3) of the Proposal specifies that "Union law on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment shall apply to personal data processed in connection with the rights and obligations laid down in this Regulation", and that the Proposal "shall not affect the applicability of Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC, including the powers and competences of supervisory authorities." Moreover, the same provision establishes that "[i]nsofar as the rights laid down in Chapter II of this Regulation are concerned, and where users are the data subjects of personal data subject to the rights and obligations under that Chapter, the provisions of this Regulation shall complement the right of data portability under Article 20 of Regulation (EU) 2016/679."

21. The EDPB and the EDPS very much welcome the objective of Article 1(3) of the Proposal, which is to ensure that the application of existing data protection rules and principles shall not be affected or undermined. In its Statement on the Digital Services Package and Data Strategy[9], the EDPB called upon the Commission to ensure legal certainty and coherence with the existing data protection framework. In particular, the EDPB encouraged the Commission to ensure that data protection rules and principles shall prevail whenever personal data are being processed.

22. The EDPB and the EDPS positively note that the compromise text of the Data Governance Act ("the DGA"), both in its recitals and enacting terms, explicitly state that in the event of conflict between the provisions of the DGA and Union law or national law on the protection of personal data adopted in accordance with Union law, the latter should prevail[10].

23. The EDPB and the EDPS strongly recommend amending Article 1(3) of the Proposal to align it with the wording of the DGA in order to enhance coherence between the Proposal, the DGA and the existing

[8] See in particular paragraph 22, and footnote 8, of the Opinion.
[9] EDPB Statement on the Digital Services Package and Data Strategy, 18 November 2021.
[10] Article 1(2a) and Recital 3a of the Draft regulation on European data governance (Data Governance Act) - text subject to revision, December 2021, available at https://www.consilium.europa.eu/en/press/press-releases/2021/11/30/promoting-data-sharing-presidency-reaches-deal-with-parliament-on-data-governance-act/

legislation on the protection of personal data. The EDPB and the EDPS consider that a reference to Regulation (EU) 2018/1725 EUDPR should be introduced in Article 1(3) and in Recital 30[11].

24. The EDPB and the EDPS consider this explicit statement necessary in light of the entities which may benefit from the right to access, use and share data generated by the use of products or related service. The Proposal assigns these rights to the 'user', who is defined as '*a natural or legal person that owns, rents or leases a product or receives a [service]'*[12]. Recital 18 clarifies that a user might be a *business or consumer* who has purchased, rented or leased the product. As result, the right to access, use and share data in practice is likely to extend to entities other than the data subject, including businesses, depending on the legal title under which the product is used[13].

25. The EDPB and the EDPS recognise that entities other than the data subject may have a legitimate reason to access data generated by the use of a product or related service. At the same time, the EDPB and the EDPS consider that there is also a significant risk that the rights to access, share or use data generated by the use of a product or related service could be exercised to unduly interfere with the rights and freedoms of data subjects. For example, an employer that has purchased virtual voice assistants and made them available to its employees could use the right to access in order to access their search history.

26. To limit the risks of an interpretation or implementation of the Proposal that could affect or undermine the application of existing data protection law, the EDPB and the EDPS call on the legislator to strengthen the wording of Article 1(3) by explicitly specifying that, in case of conflict with the provisions of the Proposal data protection law "**prevails**", insofar as it concerns the processing of personal data.

27. Finally, the EDPB and the EDPB also recommend to **clearly distinguish** in Article(s) 3, 4, 5, 6, 8 of the Proposal between the rights of data subjects to access and use data generated by their own use of products or related services and the possible rights or obligations of other actors. Access and sharing of personal data **by users other than the data subject** should **only be possible** insofar as all applicable data protection principles and rules allow such processing of personal data[14].

28. For example, the EDPB and the EDPS would welcome a Recital stating that, in accordance with the GDPR, the performance of a contract can only be a legal ground for processing of personal data if the data subject is a party or if steps are being taken at the request of the data subject prior to entering into a contract. Furthermore, this Recital should also mention that the requirement of 'necessity' is not satisfied by the mere inclusion of a contractual clause providing for the processing. The controller should be able to demonstrate how the main subject-matter of the specific contract with the data

---

[11] While Article 1(2)d of the Proposal indicates that this Regulation applies to "*public sector bodies and Union institutions, agencies or bodies that request data holders to make data available where there is an exceptional need to that data for the performance of a task carried out in the public interest and the data holders that provide those data in response to such request*" (i.e. EUIs making requests pursuant Chapter V), it does not exclude EUIs from the notion of "user" nor of the notion of "recipient". In any event, any request emanating from a EUI should also comply with the EUDPR (in addition to the requirements set forth in Chapter V).

[12] Article 2(5) of the Proposal refers to 'a services', but should be corrected to refer to the singular 'service'.

[13] See also Recital 18 of the Proposal.
Insofar as it concerns personal data, the nature of the enhanced right to data portability needs to be clarified:
in case of exercise of this right by a business, this would be about the commercial obligation for the manufacturer/data holder to provide access to data to business, subject to all conditions and limits of the GDPR, rather than a 'right' to port and have processed personal data.

subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur[15].

3.3 Interplay of the Proposal with DMA and DGA

29. The EDPB and the EDPS note that the Proposal aims at **complementing**[16] the Proposal for a **Digital Markets Act** ('DMA')[17] and the DGA[18].

30. The EDPB and the EDPS observe that **undertakings designated as gatekeepers under the DMA** shall not be eligible **third parties** for the data sharing pursuant to the Proposal[19].

31. The EDPB and the EDPS note that the Proposal **does not clarify the interplay with some key provision of the DMA** related to data sharing, notably with Article 6(1)(h)[20] and Article 6(1)(i)[21] of the DMA. In this regard, the EDPB and the EDPS recommend aligning the Proposal to the final text of the DMA agreed by the co-legislators.

32. The EDPB and the EDPS consider in particular that certain constraints on **types of data to be made available**, for instance query, click and view data (from online searches) referred to in Article 6(1)(j) of the DMA, to be made available in anonymised form[22], should also apply, *mutatis mutandis*, in the context of data sharing related to queries made to virtual assistants.

33. Having regard to the DGA, the EDPB and the EDPS remark that the Proposal includes a **different definition** than the one found in the in the DGA for the term 'data holder'[23], which may create legal uncertainty. Moreover, the definition of "data holder" in the Proposal should be further clarified[24].

34. The EDPB and the EDPS consider that the enacting terms of the Proposal should further clarify if, and subject to which conditions, a 'data recipient'[25] can be a '**provider of data sharing services**'[26] (or 'data intermediation service'[27]) as referred to in the DGA. Recital 35 refers to the case where the third party

---

[15] EDPB 2/2019 Guidelines on the processing of personal data under Article 6(1)(b) GDPR on the context of the provision of online services to data subjects Version 2.0, adopted on 8 October 2019.
[16] Explanatory Memorandum of the Proposal, pages 4 and 5.
[17] COM(2020)842 final.
[18] COM(2020) 767 final.
[19] Article 5(2) of the Proposal.
The EDPB and the EDPS also note the exclusion from the scope of the enhanced right to data portability of data generated by the use of products or related services provided by micro or small enterprises pursuant to Article 7(1).
[20] Article 6(1)(h) of the DMA Proposal, which would require gatekeepers among others to provide tools for end-users to facilitate the exercise of data portability, in line with GDPR, including by the provision of continuous and real-time access Note: at the moment of drafting, 1/4/2022, there is not yet any publically available copy of the compromise text (contrary to the DGA).
[21] Article 6(1)(i) of the DMA Proposal which would require gatekeepers to provide continuous and real-time access to and use of aggregated or non-aggregated only where directly connected with the use effectuated by the end-user in respect of the products or services offered by the relevant business user through the relevant core platform service, and when the end-user opts in to such sharing with a consent in the sense of the GDPR.
[22] See also EDPS Opinion 2/2021 on the Proposal for a Digital Markets Act, 10 February 2021, paragraph 32, page 12, "*the gatekeeper shall be able to demonstrate that anonymised query, click and view data have been adequately tested against possible re-identification risks*."
[23] The Proposal contains a definition of 'data holder' under Article 2(6); the Proposal for the DGA under Article 2(5).
[24] The meaning of "*through control of the technical design of the product and related services*" might need to be specified.
[25] As defined under Article 2(7) of the Proposal.
[26] '*data intermediation service providers*' in the Council compromise text, LIMITE, 10 December 2021 [to be checked, updated once/if a public version is available]
[27] See Article 9 of the Proposal for a Data Governance Act (DGA).

is a provider of a data intermediation service within the meaning of the DGA, and further specifies that **in this case the safeguards for the data subject provided for by the DGA apply**. However, the substance of Recital 35 of the Proposal is not mirrored by a provision in the enacting terms of the Proposal. The EDPB and the EDPS recommend **specifying the specific safeguards** for data subjects contained in the DGA that would be applicable to the data sharing from data holders to third parties as intermediaries pursuant to the Proposal. Moreover, in line with the remarks made in section 3.2, the Proposal should specify that these safeguards **complement** the ones laid down in the GDPR, as well as in the e-Privacy Directive[28], and notably in accordance with this Directive, the requirement of consent of the end-user to the data processing by the third party.

3.4 General provisions (Chapter I of the Proposal)

3.4.1 Article 1: Subject matter and scope

35. The EDPB and the EDPS note that, due to the use of very broad concepts, such as 'product' and 'related services' in Article 1(1) of the Proposal, the scope is also very broad and could benefit from more clarity[29].

36. Article 1 (4) of the Proposal states that it shall not affect Union and national legal acts providing for the sharing, access and use of data for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including Regulation (EU) 2021/784 and the [e-evidence proposals [COM(2018) 225 and 226] nor shall it affect the respective provisions of Directive(EU) 2015/849 and of the Regulation (EU) 2015/847. Finally, the competences of the Member States regarding activities concerning public security, defence, national security, customs and tax administration and the health and safety of citizens in accordance with Union law are not either affected by the proposal.

37. It is however unclear if Article 1 (4) of the Proposal has any relevant interplay with these Regulations and this Directive. To state that the Proposal does not affect these laws does not mean that data processing operations under the Proposal cannot be used for the purposes of these laws. The EDPB and EDPS recommend to further specify the possible interplays with the abovementioned legal frameworks[30].

3.4.2 Article 2: Definitions

38. The definition of 'data' under Article 2(1) of the Proposal could, depending on the nature of the data at hand, also include personal data, implying that rules in the Proposal may apply next to the GDPR. The term data is used in the Proposal indistinctively to refer to personal and non-personal data, which may lead to confusion. For instance, the reference in Recital 24 to the possibility for data holders to use data generated by the user on the basis of a contractual agreement does not clarify which type of data it refers to. If this example refers also to personal data, it is incomplete with regard to the obligations that controllers have pursuant to the GDPR, and could therefore be easily misinterpreted.

[28] ePrivacy Directive: Art. 5(3).
[29] See WP29 opinion 8/2014 on the recent developments on the internet of things, adopted on 16 September 2014.
[30] See also section 3.7 of the Opinion Regarding access to and use of data by public sector bodies and Union institutions, agencies or bodies pursuant to Chapter V of the Proposal.

39. The EDPB and EDPS therefore recommend the co-legislator to supplement Article 2 of the Proposal with a definition of 'personal data' (as defined by GDPR) and 'non personal data'. In a similar fashion, the EDPB and EDPS recommend to add definitions of 'data subject' and 'consent' into Article 2 of the Proposal, as these terms are frequently used in the Proposal and the recitals. Article 2 (5) of the Proposal defines 'user' as a natural or legal person that owns, rents or leases a product or receives a service. For the sake of clarity and to achieve an effective empowerment of individuals with regard to their personal data, the EDPB and EDPS recommend to add to this definition "and the data subject" (and to include a definition of data subject as having the same meaning as in the GDPR) as well as to clearly differentiate the situations where the user is the data subject from the situation where the user is not the data subject.

3.5 Business to consumer and business to business data sharing (Chapter II of the Proposal)

40. Chapter II of the Proposal relates to data generated by the use of products or related services. The Proposal defines a "product" as "*a tangible, movable item [...] that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data"*. A 'related service', in turn, is defined as *"a digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions*". Moreover, the Proposal clarifies in Article 7(2) that where the Proposal refers to products or related services, such reference shall also be understood to include virtual assistants[31], insofar as they are used to access or control a product or related service.

41. The EDPB and the EDPS consider that the definition of product overlaps, in part, with the **notion of *"terminal equipment"*[32] within the meaning of Article 5(3) ePrivacy Directive.** Article 5(3) of the ePrivacy Directive requires consent of the subscriber or user prior to the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or end-user, unless such storage or access is strictly necessary in order for the provider of an information society service to provide the service explicitly requested by the subscriber or user. Moreover, any processing operations of personal data following these processing operations, including processing personal data obtained by accessing information in the terminal equipment, must also have a legal basis under Article 6 GDPR in order to be lawful[33].

---

[31] Article 2(4) provides the definition of virtual assistant.

[32] According to Article 1(1)(a) of Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment, "terminal equipment" includes *"equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; [...] ".*
See also EDPB Guidelines 02/2021 on virtual voice assistants, Version 2.0, adopted on 7 July 2021, para. 25: *"In accordance with the definition of "terminal equipment", smartphones, **smart TVs** and **similar IoT devices** are **examples for terminal equipment**. Even if VVAs in themselves are a software services, they always operate through a physical device such as a smart speaker or a smart TV. **VVAs** use electronic communications networks to access these physical devices that constitute "terminal equipment" in the sense of the e-Privacy Directive. Consequently, the provisions of Article 5 (3) e-Privacy Directive apply whenever VVA stores or accesses information in the physical device linked to it*".

[33] See EDPB Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications, paragraph 41 for similar reasoning regarding connected vehicles ("EDPB Guidelines 1/2020"). See also EDPB, Opinion 5/2019 on the interplay between the e-Privacy Directive and the GDPR, in particular regarding to competence, tasks and powers of data protection authorities.

42. The EDPB and the EDPS positively note the clarification provided by Recital 15 of the Proposal, which clearly indicates that products such as personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners would not be covered by the Proposal. That being said, the EDPB and the EDPS consider that Article 2(2) of the Proposal defines a "product" in such (broad) terms that such devices might in fact fall within the scope of the definition included in the enacting terms of the Proposal. The EDPB and the EDPS therefore consider it necessary to amend the definition of "product" so as to clearly exclude products such as personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners, also in the enacting terms of the Proposal[34].

43. The EDPB and the EDPS positively note that Article 4(5) of the Proposal lays down that where the user is not a data subject, any personal data generated by the use of a product or related service shall only be made available by the data holder to the user where there is a valid legal basis under Article 6(1) of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 are fulfilled. As the Proposal assigns the right to access and use data generated by the use of products or related services to "users" (which encompasses entities other than data subjects), the EDPB and the EDPS consider that such clarification constitutes an important safeguard. As the lawfulness of processing of personal data is governed by Article 6 GDPR as a whole, however, **the EDPB and the EDPS recommend to replace the reference to Article 6(1) GDPR in Article 4(5) of the Proposal by a reference to Article 6 GDPR as a whole and more in general to all rules conditions provided by data protection legislation**. Moreover, as access to data generated by the use of products or related services may also involve access to information stored on the terminal equipment of a subscriber or user, the EDPB and the EDPS recommend clarifying that data shall only be made available by the data holder to the user on the condition that, were relevant, the conditions of **Article 5(3) ePrivacy Directive** are fulfilled.

44. The EDPB and the EDPS recall that where consent is required pursuant to Article 5(3) ePrivacy Directive, consent under Article 6 GDPR would be most probably the adequate legal basis in relation to any processing of personal data following the storing of information, or gaining access to, information already stored in the terminal equipment of a subscriber or user[35].

45. Similar considerations apply to the making available of data to third parties upon request of a business user under Article 5(6) of the Proposal. In addition, the EDPB and the EDPS recommend to further align the wording of Article 5(6) with Article 4(5) of the Proposal, by stipulating that data generated by the use of a product or related service shall only be made available "by the data holder to the third party" where all conditions and rules provided by data protection legislation are complied with, notably where there is a valid legal basis under Article 6 and where relevant, the conditions of Article 9 the GDPR and Article 5(3) of the ePrivacy Directive are fulfilled.

46. As a result, the EDPB and the EDPS stress the need to ensure that **access, use, and sharing of personal data by users other than data subjects should occur in full compliance with all the GDPR and ePrivacy obligations,** including informing data subjects about the access by controllers to their personal data and facilitating the exercise of data subject rights by controllers.

---

[34] The EDPB and EDPS wish to underline that the finding that the definition of "product" in the Proposal overlaps, in part, with the definition of "terminal equipment" within the meaning of Article 5(3) of the ePrivacy Directive, should not be understood as recommendation to revise the definition of "product" to align it with the definition of "terminal equipment".
[35] See EDPB Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications, paragraph 27.

47. Having regard, in particular, to **Article 3(1)** and 4(1) of the Proposal, the EDPB and the EDPS consider that, in order to promote **data minimisation**, products should be designed in such a way that **the data subjects** (irrespective of their legal title on the device) are offered the possibility **to use the products covered by the Proposal, in particular Internet of Bodies ("IoB") or Internet of Things ("IoT") devices anonymously** or in the least privacy intrusive way as possible. Data holders should also limit as much as possible the amount of data leaving the device (e.g. by anonymising data).[36] The Proposal should clearly specify this aspect in order to strengthen control by the data subjects on their personal data. **Article 3(2)(a)** of the Proposal, referring to the obligation to provide information to the user on the nature and volume of data likely to be generated by the use of the product, should not be interpreted as adversely affecting the GDPR data minimisation principle. Finally, the EDPB and the EDPS note that Article 3 should clearly indicate which entity/ entities shall be required to comply with the obligations listed in Article 3(1) and Article 3(2) of the Proposal. In the interest of legal certainty, the EDPB and EDPS recommend to indicate clearly which entity/entities shall be responsible for each of the obligations listed.

48. The EDPB and the EDPS note that **the limitation on keeping records** on business access to data under **Article 4(2)** and on third parties' access to data under **Article 5(3)** of the Proposal should not be interpreted as adversely affecting the GDPR obligations on security of personal data and on accountability. These provisions should clearly specify this important aspect.

49. The EDPB and the EDPS also note that, pursuant to **Article 5(9)**[37] of the Proposal, the right of the user to share data with third parties "shall **not affect data protection rights *of others***". In this regard, the EDPB and the EDPS stress the need to clarify **the scope** and the meaning of this provision. Furthermore, in order to ensure **consistency** with the right of the data subjects under Article 20 GDPR that the Proposal aims at complementing, the EDPB and the EDPS recommend referring in a Recital to the criteria for **balancing** the right to portability **with data protection concerns related to other persons** laid down in the EDPB guidelines on data portability[38].

50. **Article 6** of the Proposal specifies that third parties shall process data made available to them pursuant to Article 5 only for the purposes and the conditions agreed with the user, and subject to the rights of the data subject insofar as personal data are concerned, and shall delete the data when they are no longer necessary for the agreed purpose. Moreover, Article 6(2)(b) provides that the third party shall not use, data for profiling of data subjects, unless it is necessary to provide the service requested by the user. Having regard to the scenario of the user being an entity other than the data subject, the EDPB and the EDPS recall that it is important to ensure that **any further processing of personal data complies with Article 6(4) GDPR and, having specific regard to the profiling scenario, with the relevant obligations provided under, with Article 22 of the GDPR, where applicable.** In case of processing of special categories of personal data (e.g. such as data concerning health or sex life), explicit consent by the data subject will in principle be required, unless another exception to the prohibition contained in Article 9 GDPR can be invoked. Where Article 5(3) of the ePrivacy Directive applies, the data should only be processed with the consent of the subscriber or user, unless strictly

[36] See WP29 opinion 8/2014 on the recent developments on the internet of things, adopted on 16 September 2014.
[37] Article 4 of the Proposal should contain a similar provision having regard to Article 4(1).
[38] See WP29 (endorsed by EDPB) Guidelines on the right to data portability, at pages 11-12.

necessary in order to provide an information society service explicitly requested by the subscriber or user[39].

51. For the sake of legal certainty, and to avoid a possible interpretation according to which the relevant data protection rules in the context of the obligations to process personal data by third parties pursuant to Article 6(1) of the Proposal are only the ones referring to data subjects' rights (Chapter III of the GDPR), as also recommended in paragraphs 43 and 45 of the Opinion, the EDPB and the EDPS recommend complementing the wording in Article 6(1) referring to the GDPR "and subject to the rights of the data subject insofar as personal data are concerned", replacing it by the following: "and where all conditions and rules provided by data protection legislation are complied with, notably where there is a valid legal basis under Article 6 and where relevant, the conditions of Article 9 of the GDPR and Article 5(3) of ePrivacy Directive are fulfilled and subject to the rights of the data subject insofar as personal data are concerned."

52. Concerning Article 6(2)(a), the EDPB and the EDPS welcome the prohibition for the third party to coerce, deceive or manipulate the user in any way.[40] The EDPB and EDPS also welcome the reference to so-called 'dark patterns' in Recital 34 of the Proposal. The EDPB and EDPS note, however, that the factors that might affect decision-making may be different depending on whether or not the user is also the data subject. **The EDPB and EDPS therefore recommend making explicit that Article 6(2)(a) of the Proposal prohibits any form of coercion, deception, or manipulation of data subjects** (regardless of whether the user is also the data subject).

53. Similar considerations apply in relation to Article 6(2)(b) of the Proposal: the third party should not be allowed to use the data it receives for profiling of natural persons unless it is necessary to provide the service requested by the data subject. In addition, the EDPB and the EDPS consider that "the service" to be provided by the third party as requested by the user (which may be an entity other than the data subject) is not defined in the Proposal. It is therefore possible that such 'services' could entail a serious interference with the rights and freedoms of individuals or otherwise have a significant impact on the persons concerned.

54. Therefore EDPB and the EDPS recommend to include in the proposal clear limitations or restrictions on the use of personal data generated by the use of a product or service by any entity other than the data subject (either as "user", "data holder" or "third party"), in particular where the data at issue is likely to allow precise conclusions to be drawn concerning their private lives or would otherwise entail high risks for the rights and freedoms of the individuals concerned.

55. In particular, the EDPS and EDPB recommend to introduce limitations regarding use of personal data generated by the use of a product or related services for purposes of direct marketing or advertising, employee monitoring, credit scoring or to determine eligibility to health insurance, to calculate or modify insurance premiums. This recommendation is without prejudice to any further limitations that may be appropriate, for example to protect vulnerable persons, in particular minors, or due to the particularly sensitive nature of certain categories of data (e.g. data concerning the use of a medical device) and the protections offered by Union legislation on data protection.

[39] See also EDPB guidelines on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, adopted on 9 March 2021, paragraph 15.
[40] As specified by Recital 34, referring to so-called 'dark patterns'.

56. Moreover, the EDPB and the EDPS recall as a general principle that also third party as a controller is subject to the principle of data minimisation and that anonymisation techniques shall be used whenever possible. Compliance with the data minimisation principle is particularly important in the case of data capable of revealing intimate aspects of an individual's private life[41].

3.6 Obligations for data holders legally obliged to make data available and terms related to data access and use between enterprises (Chapter III and IV of the Proposal)

57. Chapter III addresses the conditions, including compensation, under which data shall be made available where a data holder is obliged to make data available to a data recipient as in Chapter II or in other Union law or Member State legislation.

58. In this regard, Article 8 of the Proposal foresees no role for, or reference to the data subject as terms and conditions for data sharing have to be determined in an agreement between the data holder and the data recipient. Indeed, in cases where the user is an entity other than the data subject, the latter is not part of the contract under the Proposal. This risks to severely compromise the effectiveness of data protection rights. Further risks in this context may stem from intermediation services and data brokerage, which could relate data that originally may be considered non-personal to specific data subjects[42].

59. In any case, the EDPB and the EDPS stress that the right to the protection of personal data enshrined in Article 16(1) TFEU and in Article 8 of the Charter, as a right related to each natural person, is inalienable and cannot be waived by any agreement between the data holder and the data recipient[43].

60. Pursuant to Article 8(3) of the Proposal the data holder shall not discriminate between "comparable categories of data recipients" and, as per Article 8(4) of the Proposal, the data holder cannot make data available to a data recipient on an exclusive basis. These obligations however should not undermine the right of informational self-determination of data subjects according to which they are entitled to discriminate among the recipients of their personal data (notably, when they consent to the processing, for instance in case the conditions of Article 5(3) of the ePrivacy Directive are applicable or the processing relies on consent under Article 6 GDPR). Therefore, the EDPB and the EDPS call for a wording which effectively enhances data holders' and data recipients' compliance with the GDPR. In particular, the EDPB and the EDPS recommend that the clarification provided in Recital 41 according to which these obligations are without prejudice to the GDPR is included in the text itself of Article 8.

61. Pursuant to Article 9 of the Proposal, any compensation required by the data holder to third parties has to be reasonable, and for SMEs it cannot exceed the costs incurred for making the data available, unless otherwise specified in sectoral legislations.

---

[41] See EDPB statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021, stressing "*the importance of the obligation of data protection by design and by default, which is particularly relevant in the context of 'connected objects' (e.g. the Internet of Things and the Internet of Bodies), due to the significant risks to the fundamental rights and freedoms of the persons concerned*."

[42] The more non-personal data are combined with other available information, the more the re-identification risk for data subjects increases. See EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), page 16.

[43] See the EDPB Statement on the Digital Services Package and Data Strategy adopted on 18 November 2021, page 6.

62. Regarding Article 9 of the Proposal on the compensation for making data available, the EDPB and the EDPS strongly recommend to waive any ambiguity concerning the monetary transactions accompanying the sharing of personal data. According to Recital 42 of the proposal, the right to require compensation for making data available to third parties *"should not be understood as paying for the data itself but in the case of micro, small or medium-sized enterprises, for the costs incurred and investment required for making the data available"*. This statement, however, read in conjunction with Recital 46 seems to imply that, on the contrary, in the case of data sharing between large companies, or when the data holder is a small or medium-sized enterprise and the data recipient is a large company the right for data holder to set 'reasonable compensation' to be met by third parties, may be considered as an incentive to monetise personal data.

63. In this respect, he EDPB and the EDPS reiterate that data protection is a fundamental right guaranteed by Article 8 of the Charter and personal data cannot be considered as a tradeable commodity.

64. In cases where parties disagree on the terms and conditions of making data available, the Proposal envisages alternative ways of resolving disputes that may arise between data holders and data recipients. According to Article 10 of the Proposal, these parties can seek the assistance of dispute settlement bodies certified by the Member States. However, where personal data are made available to third parties upon a request of users **who are not the data subjects**, the latter would be completely excluded from the participation to dispute settlement proceedings concerning the sharing of their personal data between the data holder and the data recipient. In addition, given the complex interactions and overlaps between the data subject's rights under the GDPR and the rights and obligation established by the Proposal, it should be taken into consideration that the parties' decision to submit a dispute to a dispute settlement body may interfere with the data subject's right to lodge a complaint with a supervisory authority.

65. More in general, the EDPB and the EDPS strongly recommend stating clearly that the dispute settlement under Article 10 shall not encroach upon data subject's rights and controllers' processor obligations established under the GDPR. In addition, paragraphs 5 and 9 of Article 10 must be amended so as to take into account that data subjects shall not be prevented from their right to seek redress before a supervisory authority.

66. The Proposal also encourages the application by the data holder of appropriate technical protection measures, including smart contracts, to prevent unauthorised access to the data and to ensure compliance with the rights and obligations arising from the proposal as well as with the agreed contractual terms for making data available (Article 11). In this regard, it should be clarified how smart contracts can constitute the means to provide data holders and data recipients with adequate guarantees that the transmitted data is prevented from unauthorised disclosure or access and that the agreed terms and conditions for sharing this data are fulfilled. In order to ensure consistency with Article 32 of the GDPR, the EDPS and the EDPB underline that to the extent that personal data is involved, paragraph 1 of Article 11 must include a reference to the obligation of implementing appropriate technical and organisational measures so as to ensure a level of security appropriate to the risk of the personal data processing.

67. Concerning Article 11(2) the EDPB and the EDPS recommend stating clearly that, insofar as it concerns personal data, the data holder's authorisation to share data cannot replace the requirement of an appropriate legal basis according to the GDPR or alternatively specifying that this authorisation applies in case of processing of non-personal data. Moreover, the same paragraph has to be amended in order to establish that any instruction from the data holder or the user (who is not necessarily the data

subject) to destroy the data made available to the data recipients and any copies thereof must not be of prejudice to the data subject's right to restriction of processing under Article 18 of the GDPR.

68. With regard to the exceptions envisaged by paragraph 3 of Article 11, the Proposal should clarify how and by whom the situations described under letter a) and b) can be judged applicable. In addition, these exceptions must take into account not only the harm to and the interests of the data holder but also and primarily the harm to the data subjects as well as their rights and interests with regard to their rights to privacy and data protection. Therefore, the EDPB and the EDPS recommend to add in Article 11 a new paragraph explicitly stating that paragraph 2(b) shall apply in case of possible harm to data subjects or prejudice to their rights and interests.

69. Finally, the reference in Article 12(1) to the data holder's obligation, under Article 5 of the Proposal, to make data available upon a user's request, suggests that as far as personal data is concerned, and despite what's said in Recital 24 when the user is an entity other than the data subject[44], the Proposal could be interpreted as creating a legal basis under Article 6(1)(c) of the GDPR for the sharing of personal data. Therefore, appropriate, specific and effective safeguards for the protection of the rights and interests of data subjects as far as personal data are concerned should be added especially where the user is not the data subject. Consequently, given the complex interactions and overlaps between the data subject's rights under the GDPR and the rights and obligation established by the Proposal, Article 12(2) of the proposal should be amended in order to specify that any contractual term in a data sharing agreement between data holders and data recipients which, to the detriment of the data subjects, undermines the application of their rights to privacy and data protection, derogates from it, or varies its effect, shall not be binding on that party.

70. In Chapter IV, Article 13 of the Proposal, the EDPB and the EDPS highlight that the Proposal state that "*a contractual term is unfair if it is of such a nature that its use grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing.*" Similarly to what is mentioned above, regarding the consistency of the definitions with the GDPR, this provision is not clear enough given the fact that the concept of personal data or non-personal data or mixed data sets is not clear throughout the text.

71. Data access and use constitute processing of personal data pursuant to Article 4(2) of the GDPR. Therefore, when personal data are involved in the processing, the obligations of the GDPR for controllers and processors shall apply. The same applies to the cases where mixed data sets (i.e. both personal and non-personal data) are involved.

72. To this purpose, the EDPB and the EDPS urge the co-legislature to clarify in the Proposal the relevant requirements and obligations of controllers and processors where personal data are processed, in the manner specified in this Opinion[45].

---

[44] Recital 5 of the Proposal when it states that the latter "should not be interpreted as recognising or creating **any legal basis for the data holder to** hold, have access to **process (personal) data**…" seems to be in contraction with Article 5 of the Proposal establishing the data holder's obligation to make data available upon a user's request, since according to the definition under Article 4(2) GDPR, the 'processing' of personal data encompasses any operation or set of operations performed on personal data or on sets of personal data, including "disclosure by transmission, dissemination or otherwise making available…".. However, if Recital 5 concerns the data processing by the data holder for its own purposes, this should be clarified.

[45] See in particular at paragraphs 39-39 and 67 of this Opinion. See also at paragraphs 43, 45, 46 and 51 of this Opinion.

3.7 Access to and use of data by public sector bodies and Union institutions, Agencies or Bodies (Chapter V)

73. As regards the 'making data available' to public sector bodies and Union institutions, agencies or bodies ('public sector bodies') based on 'exceptional need' (Chapter V of the Proposal), the EDPB and the EDPS have serious concerns on the **lawfulness**, **necessity and proportionality** of the obligation to make data available to public sector bodies and Union institutions, agencies or bodies.

74. Article 14 of the Proposal provides that, upon request, a data holder (exception made for SMEs) shall make data available to a public sector body or to Union institution, agency or body **demonstrating an exceptional need to use the data requested**. The Proposal does not refer to legislative measures to be adopted to provide the legal basis for this obligation. The EDPB and the EDPS note that Article 1(2)(d) of the Proposal refers to a task carried in the public interest.[46] In the same vein, Article 15(c) of the Proposal refers to a task carried in the public interest "*that has been explicitly provided by law*". This suggests that the Proposal envisages Article 6(1)(c) GDPR as a lawful basis for the processing carried out by the relevant public sector body, Union institution, agency or body. The EDPB and the EDPS note, however, that neither the relevant tasks of public interest, nor the public sector bodies, Union institutions, agencies or bodies who have been tasked with these missions of public interest have been clearly identified by the Proposal. Instead, the Proposal sets out a number of conditions that would give rise to a legal obligation for the data holder to provide personal data.

75. Article 17(1)(d) of the Proposal provides that, when requesting data pursuant to Article 14(1), the public sector body or Union institution, agency or body shall state in the request **the legal basis for requesting the data**. In the interest of legal certainty, the EDPB and the EDPS consider that Article 17(1)(d) should specify that the request shall clearly indicate the legal provision that explicitly assigns the task of public interest to the public sector body, Union institution, agency or body making the request.

76. Article 15 of the Proposal specifies three possible alternative scenarios where the exceptional need to use data is deemed to exist. As for cases (a) and (b) of Article 15 of the Proposal, the EDPB and the EDPS consider that the requirement "*explicitly provided by law*" should be explicitly included, since any limitation on the right to personal data must be "*provided for by law*" (Article 52(1) of the Charter, as confirmed by consolidated case law of the CJEU).

77. Limitations must be based on a legal basis that is adequately **accessible and foreseeable** and formulated with **sufficient precision to enable individuals to understand its scope**. In accordance with the principles of necessity and proportionality, the legal basis must also define the **scope and manner** of the exercise of the power by the competent authorities and be accompanied by **sufficient safeguards** to protect individuals against arbitrary interference[47].

78. Against this background, the EDPB and the EDPS observe in the first place that the **circumstances** justifying the access are not narrowly specified. The Proposal refers to "**exceptional need**", which would justify the request of data, relating to a "**public emergency**" (which is broadly defined[48]). The EDPB and the EDPS note that Recital 57 specifies that the existence of a public emergency is

[46] See also Recital (5) of the Proposal.
[47] See, among others, CJEU, C-175/20, *"SS" SIA v. Valsts ieņēmumu dienests*, ECLI:EU:C:2022:124, para. 83.
[48] Article 2(10) defines a 'public emergency' as "*an exceptional situation negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on living conditions or economic stability, or the substantial degradation of economic assets in the Union or the relevant Member State(s*)

determined according to the respective procedures in the Member States or of relevant international organisations. The EDPB and the EDPS recommend including this important specification in the operative part of the Proposal. In addition, the EDPS and EDPB consider it **necessary for the legislator to define much more stringently the hypotheses of emergency or exceptional need**. The definition of "public emergency" contained in Article 2(10) of the Proposal should therefore be amended to more clearly delineate the types of situations that would constitute a public emergency.

79. The scenario under letter (c) of Article 15 of the Proposal is actually presenting two very different use cases: a first one in which access to the data would be granted to fulfil a public interest; a second one in which access to the data would be granted to reduce administrative burden. With regard to the first use case, referring to the lack of available data prevents the public sector body from fulfilling a specific task in the public interest is **particularly problematic** having regard to the requirement of 'quality of law' (including foreseeability) providing for interferences with fundamental rights. As for the second use case, the **mere reduction of the administrative burden can difficultly outweigh the impact on the fundamental rights and freedoms of the persons concerned**. At the same time, it would not fulfil the requirement of the necessity of the interference on fundamental rights and freedoms. In this regard, the EDPB and the EDPS advocate in particular a more explicit delimitation of the circumstances in which the request can be made.

80. The EDPB and EDPS note that the **categories of personal data** to be accessed by public sector bodies are not sufficiently specified[49]. However, the obligation to provide data could extend to personal data from devices forming the IoT [50] and the IoB. Such information could concern special categories of personal data and other sensitive data such as location that would enable to draw intimate inferences on the data subject's life.

81. The EDPB and the EDPS also note that the **safeguards for data subjects** are not adequately spelled out in the Proposal. In particular, Article 17(2)(c) of the Proposal (which concerns **the content of the requests** for data by the public authority) refers to respect for the legitimate aims of the data holder, but not to the risks for the rights and freedoms *of the data subject*. According to Article 19(1)(b) of the Proposal, the public sector body *having received data* shall implement, technical and organisational measures that safeguard the rights and freedoms of the data subjects. In this regard, the EDPB and the EDPS stress that the aforesaid measures shall be taken first and foremost *at the moment of the collection* of data, rather than following data transmission.

82. Article 17(2)(d) of the Proposal specifies that the request shall concern, insofar as possible, *non-personal* data. This safeguard is accompanied by the provision under Article 18(5), according to which where compliance with the request requires disclosure of personal data, the data holder shall take reasonable efforts to pseudonymise the data, insofar as the request can be fulfilled with pseudonymised data. The EDPB and the EDPS consider that Article 18(5) should be amended so that the data holder is required to pseudonymise the data, not just "to take reasonable efforts". Therefore, the EDPB and the EDPS call the co-legislator to delete the reference to "to take reasonable efforts" since this reference seems to limit the data holder's obligation and recall that. Pseudonymisation mitigates risks for the data subjects by reducing the amount of personal data processed and the impact of an eventual data breach. In addition, the EDPB and the EDPS recommend the co-legislator to take into account that other appropriate safeguards according to the GDPR may need to be

[49] Recital 56 refers to "data held by an enterprise".
[50] Recital 14.

implemented by the data holder, notably adequate technical and organizational measures ensuring minimization, integrity and confidentiality of personal data.

83. More broadly, the EDPB and the EDPS observe that the public sector body enjoys a **broad discretion** when requesting data pursuant to the Proposal, since it is its request (and not the Proposal itself) that specifies among others: what data are required (Article 17(1)(a)); the 'exceptional need' (letter (b)), which only in case of public emergency is determined according to established procedures; the purpose of the request, as well as the intended use and the duration 'of the use' (letter c)).

84. The EDPB and the EDPS consider that the Proposal should more **clearly define the scope and manner of the exercise of the power by the public sector body** to protect individuals against arbitrary interference[51]. In particular, the EDPB and the EDPS recall that, according to case law of the CJEU[52], the legislation providing the legal basis for the measures at stake must lay down clear and precise rules governing **the scope and application** of the measure in question and imposing **minimum safeguards**, so that the persons whose personal data is affected have **sufficient guarantees** that data will be effectively protected against the risk of abuse. That legislation must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where the protection of the special categories of personal data is at stake.

85. Moreover, the EDPB and the EDPS note that according to Article 17(3) of the Proposal, public sector bodies shall **not make data available for reuse within the meaning of Directive (EU) 2019/1024**. Article 17(4), however, would allow the exchange of data between public sector bodies in the pursuit of the tasks referred to in Article 15 or the sharing of data with third parties in cases of outsourcing of 'technical inspections or other functions' by public sector bodies. Given the broad scope of Article 15, the limitation on reuse of data, including personal data, is not defined in a sufficiently narrow way. Moreover, Recital 65 of the Proposal specifies that "*Data made available to public sector bodies and to Union institutions, agencies and bodies on the basis of exceptional need should only be used for the purpose for which they were requested, unless the data holder that made the data available has expressly agreed for the data to be used for other purposes.*" The EDPB and EDPS recall that insofar as the request concerns personal data, any processing for a purpose other than that for which the personal data have been collected would be governed by Article 6(4) GDPR and/or Article 6 EUDPR, notwithstanding any expression of agreement by the data holder. Therefore, the EDPB and EDPS recommend amending the said provisions accordingly.

86. **Article 21** of the Proposal would allow further transmission of the data by public sector bodies **to natural or legal persons in view of carrying out research related to the purpose for which data was requested**. The EDPB and the EDPS recall the need for **appropriate safeguards**, taking into account

[51] See in this regard, EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19 December 2019, referring among others to the following safeguards: the notification to the person affected; the provision for the data to be retained in the European Union; the provision for the irreversible destruction of the data at the end of the retention period. See also CJEU, C-175/20, *"SS" SIA v. Valsts ieņēmumu dienests*, ECLI:EU:C:2022:124, para. 64, but also para. 83 and 84.

[52] See CJEU, C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs*, ECLI:EU:C:2020:790, para. 68.

the potentially sensitive nature of the data at issue, in accordance with Article 89 GDPR and Article 13 EUDPR.

87. The EDPB and the EDPS also recall, as indicated in the EDPB Statement on the Digital Services Package and Data Strategy, that "*particular attention should be paid to the safeguards for processing for the purposes of scientific research, ensuring lawful, responsible and ethical data management, such as* ***vetting requirements*** *for researchers who will have access to large amounts of potentially sensitive personal data*"[53]. The EDPB and the EDPS recommend integrating these requirements in the Proposal.

88. Concerning Article 18 of the Proposal, the EDPB and the EDPS consider that the reference to "sectoral legislation" (defining specific needs on the availability of data under Article 18(2)) should be specified. A specific remark concerns Article 18(6), establishing the competence of the authority referred to in Article 31 in case, among others, of challenges against the execution of the request. Since the requesting authority can be an EU Institution, agency or body, Article 31 should include the EDPS and a reference to Regulation (EU) 2018/1725. A reference should also be included in this provision to the notification of the request to the data subject and to the possibility for the data subject (not only for the data holder) to challenge the request, as well to her or his right to an effective judicial remedy against the request.

89. Concerning Article 19 of the Proposal, the EDPB and the EDPS observe that the broad definition of purposes also dilutes the safeguard under Article 19(1)(a). Moreover, the data retention period applicable depending on the purpose of the data processing should be clearly defined from the outset.

90. Article 16(2) of the Proposal specifies that "the rights from this Chapter *shall not be exercised* by public sector bodies *in order to carry out* activities for the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal penalties, or for customs or taxation administration. ''This Chapter *does not affect* the applicable Union and national law on the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal or administrative penalties, or for customs or taxation administration (emphasis added).

91. As a preliminary remark, the EDPB and the EDPS note that the provision in Article 16(2) is not aligned with Article 1(4), which specifies that the Proposal, in all its provisions, shall not affect a number of data processing activities and of competences that partially differ from the ones identified in Article 16(2). Moreover, the EDPB and the EDPS note that Recital 60 of the Proposal already confirms that public sector bodies and Union institutions, agencies and bodies should *rely on their powers under sectoral legislation* for the exercise of their tasks in the areas of prevention, investigation, detection or prosecution of criminal and administrative offences, the execution of criminal and administrative penalties, as well as the collection of data for taxation or customs purposes.

92. Given the specific nature and mission of public sector bodies and Union institutions, agencies and bodies that carry out such tasks of public interest, however, the EDPB and the EDPS consider that such entities should be excluded from the scope of Chapter V as such. Indeed, the EDPB and the EDPS consider that such entities should *only* be able to oblige data holders to make data available in accordance with the powers provided exclusively by sectoral legislation. Moreover, in particular as regards Union institutions, agencies and bodies, the EDPB and the EDPS recommend explicitly

[53] EDPB Statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021, page 7.

identifying those entities that would be able to request data in accordance with Chapter V, having due regard to the their competences as set out in their founding acts, in the enacting terms of the Proposal.

93. These recommendations are without prejudice to the need to sufficiently specify the overly broad definition of 'public emergency' in Article 2(10) that would justify the exercise of the power of access to data.

3.8 International contexts non-personal data safeguards (Chapter VII of the Proposal)

94. The EDPB and the EDPS welcome the provisions of the Proposal relating to data access which are limited to only non-personal data and seem to mirror the provisions of Article 48 of the GDPR. The EDPB and the EDPS note that in substance Article 27 primarily concerns access requests rather than transfers. The notion of "transfer" has a specific meaning under the GDPR that entails obligations to frame them. In order to avoid any confusion with respect to non-personal data, the EDPB and the EDPS suggest to refer only to access and remove the notion of transfer from this article.

95. In addition, a clarification would be useful as to the interplay between the Article 27(1) and Article 27(2) and 27(3) of the Proposal. The EDPB and the EDPS welcome the statement in article 27(1) which covers any risk of governmental access to non-personal data that would create a conflict with Union law or the national law of the relevant Member State. However, the final wording of provision, "*without prejudice to paragraph 2 or 3*" should be revised to make clear that even if there is no request, the measures provided in paragraph 1 have to be put in place in any case, i.e. irrespective of any request for access to data by a third country. Indeed, as the information regarding a request is not always available, it is important to put in place the measure to avoid such possibility of access. The EDPB and the EDPS also question whether the word "reasonable" in paragraph 1 does not reduce the impact of the measures. The EDPB and the EDPS would suggest to remove the word "reasonable" in order to ensure the efficiency of such measures or replace it by a more compelling term such as "necessary".

96. Moreover, the EDPB and the EDPS note that according to Article 27(3) of the Proposal, providers of data processing services receiving a decision to transfer or give access to non-personal data held in the Union by a court or an administrative authority of a third country may ask the opinion of competent authorities or bodies pursuant to the Proposal in order to determine whether the applicable access conditions are met. The EDPB and the EDPS welcome this provision requiring the consultation of the competent authority in specific cases. However, the consequences of the opinion of the competent authority are not specified in the provision. The EDPB and the EDPS therefore suggest to add that "*If the opinion of the competent authorities concludes that the conditions are not met, in particular because the decision concerns commercially sensitive data or affects the interests of the Union or its Member States in matters of national security or defence, then the recipient shall not provide access to the data*".

3.9 Implementation and enforcement (Chapter IX of the Proposal)

97. As a general comment regarding the provisions on governance of this Regulation, the EDPB and the EDPS would like to underline the risks posed by the Proposal which does not harmonize the supervision of the application of this Regulation between Member States, does not provide for a European consistency mechanism that could ensure the consistent application of this Regulation within the internal market, nor provides harmonized penalties, thus risking forum shopping.

98. Article 31 of the Proposal provides that each Member State shall designate one or more competent authorities as responsible for the application and enforcement of the Data Act, and that Member States may establish one or more new authorities or rely on existing authorities. The EDPB and the EDPS highlight the risk of operational difficulties that might result from the designation of more than one competent authority responsible for the application and enforcement of this Regulation. The EDPB and the EDPS have serious concerns that this draft governance architecture will lead to complexity and confusion for both organisations and data subjects, divergence in regulatory approaches across the Union and thus affect the consistency in terms of monitoring and enforcement.

99. Regarding the sectoral authorities, the provision of Article 31(2)(b) is quite vague and does not give sufficient guidance regarding the allocation of responsibilities between competent authorities, data protection authorities and sectoral authorities related to the implementation of the Proposal, thus raising a risk of overlapping and conflict of attribution. For example, the precise role of national authorities responsible for the enforcement of consumer protection (mentioned in Recital 82 and Articles 36 and 37 of this Regulation) is not defined in Chapter IX of the Proposal. The powers and tasks of the different competent authorities should be clearly defined, notably regarding the enforcement of the different provisions of the Proposal. As an example, the EDPB and the EDPS recommend that the co-legislators determine which authority shall be responsible for the application and enforcement of Chapter IV of the Proposal on unfair terms related to data access and use between enterprises. Moreover, the interplay between the governance model of the Proposal and those provided by sectoral legislations (e.g. with the competent authorities established by the Health Data Space Regulation) should be made clearer and more detailed in order to ensure legal certainty and avoid confusion.

100. The EDPB and the EDPS welcome the designation of data protection supervisory authorities as competent authorities responsible for monitoring the application of the Proposal insofar as the protection of personal data is concerned (Article 31(2)(a)). This designation is important to avoid inconsistency and possible conflict between the provisions of this Regulation and the GDPR, and to preserve the fundamental right to the protection of personal data as established under Article 16 TFEU and Article 8 of the Charter. However, the competence of the supervisory authorities is "*without prejudice to paragraph 1*". It is unclear how such provision could affect the competence of data protection supervisory authorities and sectoral authorities. Therefore, the EDPB and the EDPS call the co-legislator to modify this provision so to remove any ambiguity.

101. Moreover, it is unclear how Article 31(1) interacts with Article 31(4) of the Proposal. The Proposal provides many scenarios, which lack clarity. The EDPB and the EDPS consider that the Proposal as currently drafted could lead to conflicts of attribution, complexity for organisations and data subjects, as well as fragmented supervision between Member States. Therefore, for the sake of clarity, the EDPB and the EDPS recommend the deletion of the reference to "*without prejudice to paragraph 1 of this Article*" (Article 31(2)). The EDPB and the EDPS also strongly recommend the co-legislators to clarify Article 31(1) and 31(4) and set out clear provisions on the designation of competent, data protection, sectoral and coordinating authorities, on the attribution of responsibilities between these authorities and cooperation mechanism. Notably, the EDPB and the EDPS flag the absence of defined powers and tasks of the coordinating competent authority in the Proposal, and recommend that the co-legislator rectify that.

102. Article 31(3) of the Proposal lays down the obligation of Member States to ensure that the respective tasks and powers of the competent authorities designated pursuant to paragraph 1 of said Article are clearly defined. The EDPB and the EDPS note that many of these powers and tasks are similar with

those attributed to data protection supervisory authorities according to Article 58 of the GDPR. Nevertheless, the EDPB and the EDPS consider that Article 31(3) of the Proposal does not harmonize tasks and powers of competent authorities among Member States and the interplay between this provision and the GDPR is not clear. Furthermore, it is unclear how these tasks and powers listed in Article 31(3) of the Proposal will affect the tasks and powers exercised by the data protection supervisory authorities when monitoring the application of this Regulation insofar as the protection of personal data is concerned. It could be understood from Article 31(2)(a) that the tasks and powers of data protection supervisory authorities shall be those established by Chapter VI and VII of the GDPR. However, it is unclear whether new tasks and powers are to be assigned to these authorities by the Proposal, and if this is the case how the latter will interact with the tasks and powers assigned to the data protection supervisory authorities by the GDPR. To ensure clarity and consistency of the monitoring, the EDPB and the EDPS recommend to clearly define the envisaged role of data protection supervisory authorities in the context of the Proposal.

103. The EDPB and the EDPS welcome Article 31(6) of the Proposal, which establishes that competent authorities shall remain free from any external influence and shall neither seek nor take instructions from any other entity. In order to clarify and strengthen this provision, the EDPB and the EDPS recommend to explicitly mention the independent nature of competent authorities in the Proposal.

104. According to Article 32(1) of the Proposal, without prejudice to any other administrative or judicial remedy, natural and legal persons shall have the right to lodge a complaint, individually or, where relevant, collectively, with the relevant competent authority in the Member State of their habitual residence, place of work or establishment if they consider that their rights under this Regulation have been infringed.

105. The right to lodge a complaint pursuant to Article 32 may raise operational difficulties as it is unclear how natural or legal persons will determine if personal data are concerned and which authority is competent to handle their complaint. The EDPB and the EDPS strongly recommend that the legislator provide a clear and precise cooperation mechanism for the handling of complaints between competent authorities (i.e. data protection supervisory authorities, sectoral authorities and coordinating authorities), and establishes a clear port of entry for complainants. The EDPB and the EDPS consider that Articles 32(2) and 32(3) are insufficient, and do not provide enough information neither for complainants nor for supervisory authorities. The EDPB and the EDPS recommend that the coordinating authorities be designated as point of entry for all complaints related to this Regulation, with the task to distribute it to relevant other authorities. The EDPB and the EDPS notably recommend to explicitly mention that Chapter VIII of the GDPR is not affected by this Article.

106. It is also unclear how this Provision will interact with the one-stop-shop mechanism provided by Article 56 of the GDPR for cross-border processing as far as personal data are concerned.

107. Furthermore, the EDPB and the EDPS note the absence of specific provisions on the right to effective judicial remedy by any affected natural or legal person with regard to a failure to act on a complaint lodged with competent authorities, as well as with regard to decisions of competent authorities under this Proposal. This might lead to parallel and inconsistent regimes between the enforcement under the GDPR (for which a right to effective judicial remedy is provided) and the Proposal.

108. The EDPB and the EDPS note that Recital 82, Articles 36 and 37 of the Proposal establish the possibility to make use of the EU consumer protection cooperation network mechanism and to enable representative actions by amending the Annexes to the Regulation (EU) 2017/2394 and Directive (EU)

2020/1828. It is unclear how and to what extent the consumer protection cooperation network mechanism will interact with this Article right to lodge a complaint.

109. With regard to Article 33, the EDPB and EDPS note that the Proposal does not harmonize the penalties for infringements of the Proposal (nor specifies the violations that shall be sanctioned, the fines for the infringements of its provisions, nor the authorities or bodies competent to apply such penalties). For example, it is unclear how and which authority will be responsible for the enforcement of Article 5(2) which prohibits gatekeepers from acting as a third party with whom a user can share its data, and what penalties will be applicable. The EDPB and the EDPS recommend that the co-legislator clarifies the interplay between the Proposal and the DMA regarding the enforcement of this provision and the penalties applicable.

110. The EDPB and the EDPS notice that this provision, limiting the enforceability of the Proposal (the capability to impose harmonised sanctions), and possibly also giving raise to forum-shopping for the most lenient Member State, is prejudicial to the stated aim of the Proposal to ensure fairness in the allocation of value from data among actors in the data economy.

111. With regard to Article 34, the EDPB and the EDPS recommend that the Commission shall consult the European Data Protection Board when developing and recommending non-binding model contractual terms on data access and use, as far as personal data as concerned.

112. Finally, the EDPB and the EDPS note the absence of a European cooperation framework in the Proposal. Considering the impact of the Proposal across Member States, and the high quantity of cross-border processing that might fall under the scope of this Regulation, it is quite surprising that this Proposal does not provide a clear European cooperation mechanism in order to ensure its consistent application among Member States (especially with respect to the handling of complaints and taking into account the possible involvement of different sectoral competent authorities). The EDPB and the EDPS note that Article 31(3)(f) of the Proposal is insufficient in this sense and recommend the co-legislator to establish clear rules in order to facilitate the cooperation between the different authorities involved.

113. The EDPB and the EDPS welcome the designation of national data protection authorities as competent authorities responsible for monitoring the application of the Proposal insofar as the protection of personal data is concerned, and ask the co-legislators to also designate national data protection authorities as coordinating competent authorities under this Proposal.

114. Data protection authorities have a unique expertise, both legal and technical, in the monitoring of the compliance of data processing, in providing guidance to digital players and data subjects, and in the use of inter-regulation mechanism, placing them at the core of the digital regulation landscape.

115. Moreover, the EDPB and the EDPS are of the opinion that, considering that the GDPR applies when personal and non-personal data in a data set are inextricably linked, the role of data protection authorities should prevail in the governance architecture of this Proposal. The co-legislators should make sure that this governance reflects the prevalence of the fundamental right to the protection of personal data established under Article 16 TFEU and Article 8 of the Charter, and preserves the independence of data protection authorities.

116. The designation of coordinating competent authorities other than data protection authorities could affect consistency in terms of monitoring the application of the provisions of the GDPR and lead to real complexity for digital players and data subjects.

117. The EDPB and the EDPS note that the EDPS is only mentioned in Article 33(4) of the Proposal, which refers to penalties (for infringements of provision on public bodies' access to data, Chapter V) and is not listed as a "competent authority" in Article 31 of the Proposal. Having regard the EDPS **oversight role** as the data protection authority for the European Union institutions, bodies and agencies and the fact that some of the European Union institutions, bodies and agencies may also act as user or a data holder within the meaning of this Proposal, the EDPB and the EDPS recommend including **a reference to the EDPS as competent authority in Article 31(2)(a) for the supervision of the whole Proposal insofar as it concerns the Union institutions, bodies, offices and agencies.** Moreover, it should be clarified that, where relevant, Article 62 of Regulation 2018/1725 shall apply *mutatis mutandis*.

Brussels, 4 May 2022

For the European Data Protection Board	For the European Data Protection Supervisor
The Chair	The European Data Protection Supervisor
(Andrea Jelinek)	(Wojciech Wiewiorowski)