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)

Version 1.1

Version history

Version 1.1	09 June 2021	Minor editorial changes
Version 1.0	10 March 2021	Adoption of the Joint Opinion

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 ("EUDPR"),

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 for Data Governance Act ("the Proposal") is enacted pursuant to the Communication "A European 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, the Data Strategy provides that "*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 "*aims to foster the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU. The instrument would address the following situations:*

   - Making public sector data available for re-use, in situations where such data is subject to rights of others.

   - Sharing of data among businesses, against remuneration in any form.

   - Allowing personal data to be used with the help of a 'personal data-sharing intermediary', designed to help individuals exercise their rights under the General Data Protection Regulation (GDPR).

   - Allowing data use on altruistic grounds"[3].

4. When presenting the Proposal, the Commission has notably considered *that "the new regulation will provide a good governance framework supporting the common European data spaces and will ensure that data can be made available voluntarily by data holders. It will complement the upcoming rules on*

[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 1.

high-value datasets under the Open Data Directive which will ensure access to certain datasets across the EU for free, in machine-readable format and through standardised Application Programming Interfaces (APIs)"[4].

5. The Data Strategy also highlights that *"The availability of data is essential for training artificial intelligence systems, with products and services rapidly moving from pattern recognition and insight generation to more sophisticated forecasting techniques and, thus, better decisions*"[5].

6. As acknowledged in the Explanatory Memorandum of the Proposal*, "the interplay with the legislation on personal data is particularly important. With the General Data Protection Regulation (GDPR) and ePrivacy Directive, the EU has put in place a solid and trusted legal framework for the protection of personal data and a standard for the world"*[6].

7. The EDPB and the EDPS also point out that the Proposal, as referred to in the Explanatory Memorandum, "*aims at facilitating data sharing including by reinforcing trust in data sharing intermediaries that are expected to be used in the different data spaces. It does not aim to grant, amend or remove the substantial rights on access and use of data. This type of measures is envisaged for a potential Data Act (2021)*"[7]. At the time of drafting this Joint Opinion, the aim and content of such Data Act are not yet available.

2 SCOPE OF THE JOINT OPINION

8. On 25 November 2020, the Commission published the Proposal for a regulation of the European Parliament and of the Council on European data governance ("Data Governance Act") ("the Proposal").

9. On 25 November 2020, the Commission requested a Joint Opinion of the EDPB and the EDPS on the basis of Article 42(2) of Regulation (EU) 2018/1725 (EUDPR) on the Proposal.

10. **The Proposal is of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data. The scope of this opinion is limited to the aspects of the Proposal related to the protection of personal data, which, as observed, represent a key -if not the most important- aspect of the Proposal.**

11. In this regard, the EDPB and the EDPS notice that recital (3) provides that "*This Regulation is therefore without prejudice to Regulation (EU) 2016/679*".

12. The EDPB and the EDPS consider that the underlying objective of reinforcing trust with a view to facilitate data availability and benefit the digital economy in the EU is indeed grounded in **the need to ensure and uphold the respect and application of the EU acquis in the field of personal data**

[4] https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2103#European%20Data%20Spaces
[5] Data Strategy, pages 2 and 3.
[6] Explanatory Memorandum, page 1.
[7] Explanatory Memorandum, page 1.

protection. Applicable EU law in such field, and in particular Regulation EU 2016/679 (General Data Protection Regulation, GDPR), shall be considered as a prerequisite on which further legislative proposals may build upon without affecting or interfering with the relevant existing provisions, including when it comes to the competence of supervisory authorities and other governance aspects.[8].

13. In the view of the EDPB and the EDPS, it is therefore important to **clearly avoid in the legal text of the Proposal any inconsistency and possible conflict with the GDPR**. 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 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.

14. In particular, in this Joint Opinion, the EDPB and the EDPS point out to inconsistencies with the EU data protection legislation (as well as with other EU legislation, such as the Open Data Directive) and to problems, relating for instance to legal certainty, that would arise from the entry into force of the current Proposal.

15. Since the Proposal, as detailed in this Joint Opinion, raises a significant number of serious concerns, often intertwined, related to the protection of the fundamental right to the protection of personal data, **it is not the aim of this Joint Opinion to provide an exhaustive list of issues to be addressed by the legislators, nor always alternative proposals or wording suggestions**. Instead**, this Joint Opinion aims at addressing the main criticalities of the Proposal**. At the same time, the EDPB and the EDPS remain available to provide further clarifications and exchanges with the Commission.

16. The EDPB and the EDPS are also aware that the legislative process on the Proposal is ongoing and stress their **availability to the co-legislators to provide further advice and recommendations throughout this process**, to ensure in particular: legal certainty for natural persons, economic operators and public authorities; due protection of personal data for data subjects in line with the TFEU, the Charter of Fundamental Rights of the EU and the data protection acquis; a sustainable digital environment including the necessary 'checks and balances'.

17. This call for the involvement of data protection authorities also relates, due to the possible important links with the Proposal[9], to any forthcoming proposal for a European Data Act.

---

[8] See EDPS Opinion 3/2020 on the European strategy for data, at paragraph 64: "Finally, the EDPS underlines that in the context of future governance mechanisms the competences of the **independent supervisory authorities for data protection** must be properly respected. Moreover, the implementation of the Strategy leading to wider use of data will require a **significant increase of resources for DPAs** and other public oversight bodies, in particular in terms of **technical expertise and capabilities**. Cooperation and joint investigations between all relevant public oversight bodies, including data protection supervisory authorities, should be encouraged."

[9] The Impact Assessment accompanying the Proposal, SWD (2020) 295 final, specifies at page 6 that (bold added): "The current initiative is **a first step in the two-step approach** announced in the European Strategy for Data. **The initiative** will address the urgent need to facilitate data sharing through an enabling **governance framework**. **In a second step**, the Commission will address issues about **who controls or 'owns' the data, i.e. the material rights on who can access and use what data under which circumstances**. The **introduction of such rights** will be examined in the context of the **Data Act (2021)**. Diverging interests of the stakeholders and

3 ASSESSMENT

3.1 General remarks

18. The EDPB and the EDPS acknowledge the legitimate objective of fostering the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU, while highlighting that the protection of personal data is an essential and integral element of the trust individuals and organizations should have in the development of the digital economy. The proposal for a regulation on European Data Governance (Data Governance Act) is also to be considered in the light of the increased reliance of the digital economy on the processing of personal data and of the development of new technologies such as large data set analytics and artificial intelligence.

19. The EDPB and the EDPS underline that, whereas the GDPR was built upon the need to reinforce the fundamental right to data protection, the Proposal clearly focuses on unleashing the economic potential of data re-use and sharing. Thus, the Proposal intends to "improve the conditions for data sharing in the internal market", as stated in Recital (3). However, **the EDPB and the EDPS note that the Proposal, also having regard to the Impact Assessment accompanying it, does not duly take into account the need to ensure and guarantee the level of protection of personal data provided under EU law. The EDPB and the EDPS consider that this policy trend toward a data-driven economy framework without a sufficient consideration of personal data protection aspects raises serious concerns from a fundamental rights viewpoint.** In this regard, the EDPB and the EDPS emphasise that any proposal, including upcoming initiatives related to data, such as the European Data Act, that may have an impact on the processing of personal data, must ensure and uphold the respect and application of the EU acquis in the field of personal data protection.

20. **The EDPB and the EDPS furthermore highlight that the European Union model relies on the mainstreaming of its values and fundamental rights within its policy developments, and that the GDPR must be considered as a foundation on which to build a European data governance model. As already stated in various policy contexts, such as the fight against the COVID-19 pandemic, the EU legal framework in the field of personal data protection shall be considered as an enabler, rather than an obstacle, to the development of a data economy that corresponds to the Union values and principles.**

21. The EDPB and the EDPS trusts this Joint Opinion will inform the co-legislators in ensuring the adoption of a legislative instrument which is fully compliant with the EU acquis in the field of personal data protection and therefore increases trust by upholding the level of protection provided by EU law under the supervision of the independent Data Protection Authorities established under Article 16(2) TFEU.

---

different views on what is fair in this respect make these issues subject to intense debate, which warrants taking more time."

3.2 General issues related to the relationship of the Proposal with Union law in the field of personal data protection

22. The Proposal contains several references to compliance with the GDPR – which lays down the rules relating to the protection of natural persons with regard to the processing of personal data and to the free movement of personal data (see, among others, recital (3); recital (28) of the Proposal: *"when the data sharing service providers are data controllers or processors in the sense of Regulation (EU) 2016/679 they are bound by the rules of that Regulation.*").

23. The EDPB and the EDPS consider that, in light of the scope of the processing of personal data to which the Proposal makes reference, recital 3 should also include a reference to Directive (EC) 2002/58 ("ePrivacy Directive"), as it is also part of the EU acquis in the field of personal data protection with which the Proposal shall be in compliance, consistent.

24. More in general, the EDPB and the EDPS consider that **both the spirit and the letter of the Proposal must not undermine the level of protection and ensure full consistency with all the principles and rules** established by the GDPR to effectively guarantee the fundamental rights to the protection of personal data provided under Article 8 of the Charter and Article 16 TFEU.

25. Having regard to the above, as referred to in the following paragraphs of this Joint Opinion, the EDPB and the EDPS consider that **the Proposal raises significant inconsistencies with the GDPR**, as well as with other Union law[10], in particular as regards the following five aspects:

(a) Subject matter and scope of the Proposal

(b) Definitions/terminology used in the Proposal;

(c) Legal basis for the processing of personal data;

[10] Although this observation does not strictly relate to the processing of personal data, the EDPB and the EDPS also notice possible confusion and ambiguities as to how the Proposal will apply together with the **Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union**. In this regard, it should be pointed out that the definitions of 'processing', 'user', 'professional user', and 'data localization requirement', as well as to other provisions of the Regulation on non-personal data (see for instance Article 6, *Porting of data*), might be not **consistent** or however overlapping with the definitions and the other provisions contained in the Proposal. Moreover, with regards to the re-use of data held by public sector bodies which are protected on grounds of statistical confidentiality, it should be pointed out that, despite the principle stated by Article 3(3) of the Proposal, the conditions for re-use defined in Article 5(3-4) are not in line with the sectoral rules established at EU level for the protection of confidential data used for statistical purposes (see Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities and the Commission Regulation (EU) No 557/2013 of 17 June 2013 implementing Regulation (EC) No 223/2009 of the European Parliament and of the Council on European Statistics as regards access to confidential data for scientific purposes and repealing Commission Regulation (EC) No 831/2002.

(d) Blurring of the distinction between (processing of) personal and non-personal data (and unclear relationship of the Proposal with the Regulation on free flows of non-personal data);

(e) Governance/tasks and powers of competent bodies and authorities to be designated in accordance with the Proposal, having regard to the tasks and powers of data protection authorities responsible for the protection of the fundamental rights and freedoms of natural persons in relation to the processing of personal data as well as for facilitating the free flow of personal data within the Union.

A. Subject matter and scope

26. According to Article 1(2) of the Proposal: "*This Regulation is without prejudice to specific provisions in other Union legal acts regarding access to or re-use of certain categories of data, or requirements relating to processing of personal or non-personal data.*

Where a sector-specific Union legal act requires public sector bodies, providers of data sharing services or registered entities providing data altruism services to comply with specific additional technical, administrative or organisational requirements, including through an authorisation or certification regime, those provisions of that sector-specific Union legal act shall also apply."

27. **For the sake of clarity, the EDPB and the EDPS recommend introducing in Article 1 of the Proposal a provision clearly and unambiguously stating that the Proposal leaves intact and in no way affects the level of protection of individual with regard to the processing of personal data under the provisions of Union and national law and that the Proposal does not alter any obligations and rights set out in the data protection legislation. This addition would provide for better legal certainty and guarantees that fundamental right to the protection of personal data is not undermined.**

28. In this regard it is unclear why a similar specification is contained in Article 9(2) of the Proposal referring to data sharing service providers[11] and not (*mutatis mutandis*, that is referring also to public sector bodies, re-users, data altruism organisations) as a horizontal provision under Article 1 of the Proposal.

B. The definitions of the Proposal are inconsistent with the definitions and key concepts of the GDPR, and therefore need to be amended or clarified

29. The definition of *"data holder"* provided under Article 2(5) of the Proposal: "*the legal person or data subject who, in accordance with applicable Union or national law, has the right to grant access or to share certain personal or non-personal data under its control*" is not in line with the overarching principles of the GDPR, as well as with the letter of the GDPR.

30. In this regard, the EDPB and the EDPS note that legal uncertainties may arise from the fact that the GDPR does not mention the data subject's right to grant access or to share his/her personal data with

[11] Article 9(2) states: "*This Chapter shall be without prejudice to the application of other Union and national law to providers of data sharing services, including powers of supervisory authorities to ensure compliance with applicable law, in particular as regard the protection of personal data and competition law*".

third parties and even less so an equivalent right for the legal person which seems possible to extrapolate from the definition of "data holder". Rather, the GDPR guarantees to every individual the right to the protection of personal data concerning him or her, which refers to a comprehensive set of rules for the processing of personal data that are binding for each entity processing the data (data controller/joint controller) or processing the data on behalf of the data controller (processor)[12].

31. **In this regard, the EDPS and the EDPB believe that rather than stating that a legal person has the right to grant access to or share personal data, it would be more appropriate referring to whether and under which conditions a certain processing of personal data can be performed or not.**

32. A clarification that the EDPB and the EDPS would like to make is that both the access to and the sharing of personal data constitute processing of personal data pursuant to Article 4(2) of the GDPR.

33. According to the data protection legislation, the processing of personal data shall be lawful if the data subject (the identified or identifiable natural person to whom personal data relate) has given consent to the processing of his or her personal data for one or more specific purposes or if another adequate legal basis under Article 6 GDPR can be validly applied.

34. The aforesaid considerations are made in the light in particular of Article 8 of the Charter: "*1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law*."

35. The EDPB and the EDPS have concerns also as regards the wording of recital (14) of the Proposal (underline added): "*Companies and data subjects should be able to trust that the re-use of certain categories of protected data, which are held by the public sector, will take place in a manner that respects their rights and interests*."; Article 11(6), referring to "*guarantees in place that allow data holders and data users to obtain access to their data in case of insolvency*"; as well as of Article 19, "*Specific requirements to safeguard rights and interests of data subjects and legal entities as regards their data*", which refers under Article 19(1)(a) to: "*the purposes of general interest for which it [any entity entered in the register of recognised data altruism organisations] permits the processing of their data [of data holders] by a data user".*

36. In this regard, the EDPB and the EDPS remark that rights and interests of the data subject with regard to his or her personal data, on the one hand, and the right and interests of legal persons with regard

[12] See also recital (6) and (7) of the GDPR (bold added):
"(6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a **high level of the protection of personal data**.
(7) Those developments require a **strong and more coherent data protection framework** in the Union, backed by **strong enforcement**, given the importance of creating the **trust** that will allow the digital economy to develop across the internal market. **Natural persons should have control of their own personal data**. **Legal and practical certainty** for natural persons, economic operators and public authorities should be enhanced."

to the information relating to them, on the other hand, are not of the same kind (the latter does not concern human dignity or the right to privacy and to data protection, but rather industrial property rights, such as trade secrets, patents and trademarks). Therefore, given the aforesaid heterogeneity, the mentioned provisions would be not only not conceptually 'solid', but also difficult to implement and such as to raise legal uncertainties. For instance, in case of insolvency (referred to under Article 11(6)), the guarantees in place to allow data holders to obtain access to non-personal data would differ substantially in practice from conditions and limits for the continued processing of personal data. These are indeed different issues that require different solutions[13], and the reference to both under the obligation for the data sharing service provider to ensure continuity of provision of services (including the sharing of personal data) is confusing at least, if not manifestly inconsistent with the GDPR.

37. The definition of 'data user'[14] under Article 2(6) is also a new definition introduced by the Proposal, whose interplay -in case of personal data- with the definition of recipient[15] under Article 4(9) of the GDPR is unclear. We note in this regard that Article 11(1) of the Proposal lays down: "The provider may not use the data for which it provides services for other purposes than to put them at the disposal of data users [...]" This provision, read in conjunction with the definition of 'data user', gives rise to legal uncertainty, due to different notions of *'recipient'* under GDPR and *'data user'* under the Proposal, which would lead to difficulties of practical application. Moreover, the definition under Article 2(6) might be misleading if read as referring to a natural or legal person that is authorised (has the right?) to use personal data for commercial and non-commercial purposes. The reference to and the meaning (its legal source and effect) of such "authorization" is also unclear.

38. In addition, the interplay between the notion of data user as "natural or legal person [authorised to use data for commercial and non-commercial purposes]" and the notions of controller, joint controller or processor under the GDPR is also unclear. Furthermore, the Proposal refers to a possible qualification as controller or processor and their obligations under the GDPR for the data sharing service providers[16], but not for the data user or for the data altruism organisations (despite the fact that the latter can also be controller, joint controller or processor under the GDPR).

39. **More in general, the EDPB and the EDPS underline that the Proposal should define the roles in respect of personal data protection law (data controller, processor or joint controller) of each type of 'actor' (data sharing service provider, data altruism organisation, data user) not only to avoid**

---

[13] For instance, in case of insolvency, attention should be paid to the fact that, as a result, there is a change in the controllership of the data processing. The new controller shall establish in particular what data can be processed; identify the purposes for which the data was originally obtained; establish the lawful basis for sharing the data; ensure compliance with the data protection principles, in particular lawfulness, fairness and transparency; inform data subjects about changes relating to the processing of their data, and consider that data subjects may exercise their right to object.

[14] Article 2(6) of the Proposal: "'**Data user**' means **a natural or legal person** who has lawful access to **certain** data and is **authorised to use that data** for commercial or non-commercial purposes."

[15] According to the definition provided in the GDPR, under Article 4(9), "'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not [..]".

[16] See recital 28 "where the data sharing service providers are data controllers or processors in the sense of the Regulation (EU) 2016/679 they are bound by the rules of that Regulation."

ambiguity about the applicable GDPR obligations, but also to improve the readability of the legal text.

40. Similar issues, namely the **unclear relationship with the definitions and rules provided under the GDPR**, relate to the definition of 'data sharing' under Article 2(7) of the Proposal (referring *inter alia* to the 'joint or individual use of the shared data'). Insofar as it relates to personal data, the joint use of personal data (by both the data holder, legal person, and a data user) directly or through an intermediary, is also confusing at least.

41. Similar concerns - as further detailed below - relate to the term "permission [from legal entities to the reuse of data]", for which however a definition is not provided in the Proposal.

42. The definition of 'metadata' in Article 2(4) is also problematic under the personal data protection viewpoint, since it refers to "data collected on any activity of a natural or legal person for the purposes of the provision of a data sharing service, including the date, time and geolocation data, duration of activity, connections to other natural or legal persons established by the person who uses the service". Such data may include personal data.

43. As further detailed in this Joint Opinion, having regard to Article 11(2), the Proposal may be interpreted as creating a legal basis for the processing of metadata. Article 11 of the Proposal seems to lay down that, as a condition for providing the data sharing service, the provider should indeed be able to use the aforesaid metadata "for the development of that [the data sharing] service". No reference is made in the legal text among others to the need for the data sharing service provider to rely upon an appropriate legal basis for processing of personal data under Article 6(1) of the GDPR.

44. **More in general, the EDPB and the EDPS consider that since the Proposal is, as made explicit in the Proposal itself, without prejudice to the GDPR, the definitions envisaged by the GDPR should apply and they should not be implicitly amended or removed by the Proposal and the new definitions, as far as they relate to the processing of personal data, should not, as 'a matter of fact', contain 'rules' that are inconsistent with the spirit and the letter of the GDPR.**

45. This specification is particularly important due to the cumulative effect in terms of lack of clarity and legal uncertainties arising from the Proposal where more than one unclear definition is contained in the same provision (see for instance Article 7(2)(c) of the Proposal, referring to "obtaining consent *or* permission by re-users for re-use for altruistic and other purposes in line with specific decisions of data holders").

46. **In light of the above, the EDPB and the EDPS recommend clarifying and modifying the Proposal in order to ensure that -insofar as personal data are concerned- no inconsistencies with the definitions and concepts of the GDPR remain.**

C. The Proposal should better specify, to avoid legal uncertainties, the applicable legal basis in the GDPR for the processing of personal data

47. The EDPB and the EDPS notice that the Proposal makes reference to "the permission of data holders" for the use of data under several provisions:

- Article 5(6): "*the public sector body shall support re-users in seeking consent of the data subjects and/or permission from the legal entities whose rights and interests may be affected by such re-use", specified under recital (11): "The public sector bodies, where relevant, should facilitate the re-use of data on the basis of consent of data subjects or permissions of legal persons on the re-use of data pertaining to them through adequate technical means."*

- Article 7(2)(c): *"assisting the public sector bodies, where relevant, in obtaining consent or permission by re-users for re-use for altruistic and other purposes in line with specific decisions of data holders [..]";*

- Article 11(11): *"where a provider provides tools for obtaining consent from data subjects or permissions to process data made available by legal persons";*

- Article 19(3): "*Where an entity entered in the register of recognised data altruism organisations provides tools for obtaining consent from data subjects or permissions to process data made available by legal persons", specified under recital (36) "Legal persons could give permission to the processing of their non-personal data for a range of purposes not defined at the moment of giving the permission."*

48. The EDPB and the EDPS notice in this regard that it is unclear in most cases whether the object of the permission would be the re-use of personal or non-personal data or both.

49. The EDPB and the EDPS also remark that in case of processing of personal data **the "permission" referred to in the Proposal cannot replace the necessity of one appropriate legal ground under Article 6(1) of the GDPR for the lawful processing of personal data**. In other words, according to the GDPR the processing of personal data shall be lawful only if and to the extent that at least one of the legal basis under Article 6(1) of the GDPR applies. The Proposal should clearly specify this aspect to avoid any ambiguity.

50. Indeed, even interpreting the notion of 'permission', (to be however defined in the legal text of the Proposal) as 'a decision (a business choice) by a legal person to permit the processing of personal data where such legal person has a legal basis under Article 6(1) of the GDPR to permit such processing', it has to be noted that the literal reading of some provisions of the Proposal does not seem to support this GDPR-compliant interpretation, since they refer for instance to "*Where the re-use of data cannot be granted in accordance with the obligations laid down in paragraphs 3 to 5 and there is no other legal basis for transmitting the data under Regulation (EU) 2016/679, the public sector body shall support re-users in seeking consent of the data subjects and/or permission from the legal entities*" (Article 5(6) of the Proposal)[17]. In these cases, 'permission' seems to be alternative to at least one (consent of the data subject) of the legal basis provided under Article 6 of the GDPR.

51. Recital 6 of the Proposal is also unclear with regard to the appropriate legal basis for the processing of personal data, since it refers to an obligation "in general" to rely on the legal basis provided in Article 6 of the GDPR for the processing of personal data[18].

[17] See also Article 7(2)(c); Article 11(11); Article 19(3) of the Proposal referred to above

[18] In particular, recital 6 of the Proposals states that (bold added): "**In general**, insofar as personal data are concerned, the processing of personal data should rely upon one or more of the grounds for processing provided in Article 6 of Regulation (EU) 2016/679."

52. From another standpoint, as a further detailed in this Opinion, the EDPB and the EDPS remark the need to **clarify the relationship between the different scenarios envisaged under the Proposal and Article 6(4) of the GDPR**, regulating the situation where the processing of personal data for a purpose other than that for which the personal data have been collected is not based on the data subject's consent.

53. **To that effect, in light of the objective and content of the Proposal, the EDPB and the EDPS consider that the Proposal cannot be invoked as Union law constituting a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1) of the GDPR in order to ground the processing for a purpose other than that for which the personal data has been initially collected, where such processing is not based on consent, as per Article 6(4) of the GDPR.**

54. **Also in light of the above, the EDPB and the EDPS recommend specifying in the legal text of the Proposal that insofar as personal data are concerned, their processing must always be based on an adequate legal basis under Article 6 of the GDPR.**

55. As an example of possible inconsistency relating to the legal basis for the processing of personal data, we point out to the provision under Article 11(2) of the Proposal, according to which *"the metadata collected on the basis of the data sharing offered may be used [only] for the development of the data sharing services"*. In this regard, we recall that metadata referred to in the Proposal[19] can constitute information relating to an identified or identifiable natural person and in this case must be processed in accordance with data protection rules and, in particular, those concerning the legal basis of the processing. However, as referred to in paragraph 51 of this Opinion, this essential aspect is not addressed by the Proposal.

56. **On this matter, as a broader observation, the EDPB and the EDPS consider that the aforesaid provision, as well as any other provision of the Proposal, does not provide a self-standing legal basis for the re-use of personal data by data users and for the processing activities performed by providers of data sharing services or by data altruism organisations, due to the fact that it does not fulfil the criteria under Article 6(3) for the processing referred to in point (c) and (e) of Article 6(1)[20] of the GDPR.**

---

[19] Under Article 2(4) of the Proposal "'metadata' means data collected on any activity of a natural or legal person for the purposes of the provision of a data sharing service, including the date, time and geolocation data, duration of activity, connections to other natural or legal persons established by the person who uses the service."

[20] "3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:
(a) Union law; or (b) Member State law to which the controller is subject.
The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the

D. Blurring of the distinction between (processing of) personal and non-personal data and unclear relationship of the Proposal with the Regulation on free flows of non-personal data

57. As a general remark, the EDPB and the EDPS consider that a main criticality of the Proposal, having regard to the protection of personal data, possibly at the origin of the aforesaid incompatibilities or at least ambiguity of the legal text, is the blurring of the distinction between the processing of non-personal data, as regulated for certain aspects under Regulation (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union ("Regulation on the free flow of non-personal data)"[21], and the processing of personal data, the latter regulated under the data protection acquis and inspired by different principles.

58. In this regard, the EDPB and the EDPS underline that the distinction between categories of personal and non-personal data is difficult to apply in practice. Indeed, in practice, from a combination of non-personal data it is possible to infer or generate personal data, i.e. data relating to an identified or identifiable individual[22], especially when non-personal data are the result of the anonymisation of personal data and thus information originally related to natural persons. In addition, in the scenarios envisaged by the Proposal of increased availability, re-use and sharing of information, with a view to "allowing 'Big Data' pattern detection or machine learning"[23], the more non-personal data are combined with other available information, the more difficult it will be to ensure anonymisation because of the increased re-identification risk for data subjects. Consequently, having this scenario in mind, the data subjects' fundamental rights to privacy and data protection should be ensured in any case in the different contexts envisaged by the Proposal.

59. At the same time, there might be cases of non-personal data, to which the GDPR does not apply, that since their origin, do not relate to naturals persons. For instance, it is the case of non-personal data from vibration sensors in industrial machinery combined with other non-personal data, e.g. the geolocation of the machinery. Such non-personal data does not need the same level of safeguards than non-personal data that are the result of the anonymisation of personal data, as only the latter (likewise pseudonymised data) are likely to be exposed to the risk of re-identification.

60. **To avoid confusion as to how the Proposal would apply 'together with the GDPR', the EDPB and the EDPS recommend reworking the Proposal taking better into account the distinction between personal and non-personal data as well among different types of non-personal data.**

Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued."

[21] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.), OJ L 303, 28.11.2018, p. 59–68.

[22] See EDPS Opinion 3/2020 on the European strategy for data at para 30.

[23] Explanatory Memorandum, page 3.

61. Therefore, notwithstanding the concerns already expressed by the EDPS with regard to the concept of mixed dataset and to "inextricably linked" personal and non-personal data[24], the EDPB and the EDPS recall that, according to Article 2(2) of the Regulation on the free flow of non-personal data: "*In the case of a data set composed of both personal and non-personal data, this Regulation applies to the non-personal data part of the data set. Where personal and non-personal data in a data set are inextricably linked, this Regulation shall not prejudice the application of Regulation (EU) 2016/679*." Consequently, a mixed dataset will as a rule be subject to the obligations of data controllers and processors and the data subject's rights established by the GDPR. This consideration is particularly relevant in the context of the Proposal, since it is possible that in most cases datasets shared through a data sharing service provider or a data altruism organisation would also contain personal data. Since a 'third category' between personal and non-personal data does not exist, this would not change the nature and the 'legal regime' of the dataset as personal data[25].

62. **In the light of the above, the EDPB and the EDPS point out to the risk that the Proposal creates a parallel set of rules, which are not consistent with the GDPR, nor with the Regulation on the free flow of non-personal data, thus undermining it and causing difficulties of practical application.**

E. Governance/tasks and powers of competent bodies and authorities to be designated in accordance with the Proposal and tasks and powers of the data protection authorities

63. The Proposal foresees the designation by Member States of competent bodies to support the public sector bodies which grant access to the re-use of data (Chapter II of the Proposal) and the designation of competent authorities to monitor the compliance with the provisions related to data sharing services and data altruism (Chapters III and IV of the Proposal).

64. **As a broader remark, the EDPB and the EDPS are of the opinion that, since many of the tasks of the competent bodies and authorities under the Proposal relate to the processing of personal data, there is a risk of interferences by the competent bodies and authorities designated under the Proposal with the competence and tasks of independent data protection authorities. Therefore, the designation of competent authorities/bodies other than data protection authorities could lead to real complexity for digital players and data subjects, and also affect consistency in terms of monitoring the application of the provisions of the GDPR. The designation of competent bodies and authorities being left at the discretion of Member States, there may also be a risk of inconsistency and divergence in regulatory approaches across the Union.**

---

[24] See the Comments of the EDPS on a Proposal for a Regulation of the European Parliament and of the Council on a framework for the free-flow of non-personal data in the European Union issued on the 8th June 2018 at https://edps.europa.eu/sites/edp/files/publication/18-06-08-edps_formal_comments_freeflow_non_personal_data_en.pdf.

[25] See also Communication from the Commission to the Council and to the European Parliament, *Guidance on the Regulation on a framework for the free flow of non-+persona data in the European Union*, at: https://ec.europa.eu/digital-single-market/en/news/guidance-regulation-framework-free-flow-non-personal-data-european-union

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

3.3.1 Relationship of the Proposal with the Open Data Directive and with the GDPR

65. While the Explanatory Memorandum states that the Proposal *"complements the Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (Open Data Directive)*[26]*"*, recital (5) further specifies that "*Directive (EU) 2019/1024 as well as sector-specific legislation ensure that the public sector makes more of the data it produces easily available for use and re-use. However, certain categories of data (commercially confidential data, data subject to statistical confidentiality, data protected by intellectual property rights of third parties, including trade secrets and personal data not accessible on the basis of specific national or Union legislation, such as Regulation (EU) 2016/679 and Directive (EU) 2016/680) in public databases is often not made available, not even for research or innovative activities. Due to the sensitivity of this data, certain technical and legal procedural requirements must be met before they are made available, in order to ensure the respect of rights others have over such data. Such requirements are usually time- and knowledge-intensive to fulfil. This has led to the underutilisation of such data. While some Member States are setting up structures, processes and sometimes legislate to facilitate this type of re-use, this is not the case across the Union."*

66. The EDPB and the EDPS observe that, despite the aforesaid specifications, the interface of the Proposal with the "Open Data Directive" seems unclear. In particular, there might be legal uncertainty on the extended re-use of public sector information, which, according to Article 3 (Categories of data) of the Proposal, would apply to:

"*[..]data held by public sector bodies which are protected on grounds of:*

(a) commercial confidentiality;

(b) statistical confidentiality;

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

(d) protection of personal data."

67. The Explanatory Memorandum to the Proposal[27] does not sufficiently clarify the scope of such extended re-use and the interplay of the Proposal with the Open Data Directive. Moreover, it puts under the same 'umbrella' (as "*respect of rights of others*", which is inappropriate having regard to

[26] OJ L 172, 26.6.2019, p. 56–83.

[27] See at page 7: *"Chapter II creates a mechanism for **re-using certain categories of protected public sector data,** which is **conditional on the respect of rights of others** (notably on grounds of protection of personal data, but also protection of intellectual property rights and commercial confidentiality). This mechanism is without prejudice to sector-specific EU legislation on access to and the re-use of this data. **The re-use of such data falls outside the scope of Directive (EU) 2019/1024** (Open Data Directive). Provisions under this Chapter do not create right to re-use such data, but provide for a set of harmonized basic conditions under which the reuse of such data may be allowed (e.g. the requirement of non-exclusivity)."*

the protection of personal data) "*protection of personal data, but also protection of intellectual property rights and commercial confidentiality*".

68. It can be argued that the wording "*data held by public sector bodies which are protected on the grounds of*", among others *"protection of personal data"* (Article 3, letter (d)) is at the same time:

- regrettable, since it suggests the idea of data protection regulation as *impeding* the free movement of personal data, rather than laying down the rules of free flow of personal data while protecting the rights and interests of the persons concerned; *and*

- partially inaccurate, since the Open Data Directive, rather than excluding personal data from its scope[28], provides, under Article 1(2)(h), that [the Open Data Directive does not apply to] *"documents, access to which is excluded or restricted by virtue of the access regimes on grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data or as undermining the protection of privacy and the integrity of the individual, in particular in accordance with Union or national law regarding the protection of personal data*"[29].

69. This last aspect is however specified under recital 7 of the Proposal[30]. In this regard, the EDPB and the EDPS wonder why this important issue (as well as many others concerning the protection of personal data) is included in a recital, but not in the substantive part of the Proposal.

70. Moreover, pursuant to Article 3(1) of the Open Data Directive, personal data that do not fall under this exception, being freely accessible according to the Union or national access regimes and re-usable for compatible uses without undermining the protection of privacy and the integrity of the individual, are within the scope of the Directive and can be made available for re-use in accordance to the conditions set out in the same Directive as well as in compliance to the requirements of data protection law . Indeed, as stated in recital 154 of the GDPR, the EU legislation on the re-use of public sector information *"leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in [the GDPR]".* To this effect, the EU legislator when establishing new principles and rules for the re-use of public sector information should provide for the necessary reconciliation of such re-use with the right to the protection of personal data pursuant to the GDPR[31].

71. **Consequently, the EDPB and the EDPS underline that the rules of the Open Data Directive along with those of the GDPR provide already for mechanisms allowing the sharing of personal data held by**

---

[28] See Article 1 of the Open Data Directive.
[29] See also in this regard, recital 52 and 53 as well as Articles 1(4) and 10 of the Open Data Directive, the latter with specific reference to research data.
[30] *"The data covered by this Regulation* ***fall outside the scope of Directive (EU) 2019/1024*** *that excludes data subject to commercial and statistical confidentiality and data for which third parties have intellectual property rights.* ***Personal data fall outside scope of Directive (EU) 2019/1024 insofar as the access regime*** *excludes or restricts access to such data for reasons of privacy and the integrity of the individual, in particular in accordance with data protection rules."* (emphasis added).
[31] See recital 154 as well as Article 86 of the GDPR with specific reference to Union and Member State law on public access to official documents

the public sector bodies in a manner consistent with the requirements governing protection of individuals' fundamental rights. Thus, the EDPB and the EDPS recommend to align Chapter II of the Proposal with the existing rules on the protection of personal data laid down in the GDPR and with the Open Data Directive, so as to ensure that the level of personal data protection in the EU is not undermined and to avoid, at the same time, that these misalignments generate legal uncertainty for individuals, public sector bodies and re-users. As an alternative, without prejudice to the further indications in this Joint Opinion about the impact on the individuals' right to privacy and data protection of the rules of the Proposal governing the re-use of certain categories of protected data held by public sector bodies, personal data could be excluded from its scope.

3.3.2 Article 5: conditions for re-use of data by public sector bodies

72. The conditions for re-use of data held by public sector bodies are provided under Article 5 of the Proposal as specified under recital 11. In this regard, the EDPB and the EDPS consider that the Proposal raises some concerns.

73. **The EDPB and the EDPS reiterate that all processing of personal data as referred to in the Proposal shall occur in full compliance with the GDPR, and thus accompanied by appropriate data protection safeguards. This means that the re-use of personal data should always respect the principles of lawfulness, fairness and transparency as well as purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality in line with Article 5 of the GDPR.**

74. In this scenario, fairness, transparency and purpose limitation are essential safeguards to bring trust among individuals whose personal data are held by the public sector, making them confident that the re-use of the information they provide will take place in a manner that respects their rights and interests (see recital 14 of the Proposal), i.e., that their personal data will not be used against them in an unexpected manner. The importance of the principle of purpose limitation is clearly demonstrated in the context of the measures that are being considered to fight against the COVID-19, e.g. health data to be processed under the control of healthcare authorities as data controllers and not to be used for commercial or other incompatible purpose[32]. Consequently, public sector bodies which are competent under national or EU law to grant or refuse access for the re-use must take into account that the re-use of personal data is permissible only if the principle of purpose limitation as set out in point (b) of Article 5(1) and Article 6 of the GDPR is met[33]. Any subsequent use of data, collected and/or shared in pursuit of a public task (e.g. for improving transport/mobility or tackling serious cross-border threats to health), for commercial for-profit purposes (for instance insurance, marketing, etc.) should be avoided. Such "function creep" might not only constitute a breach of the data protection principles under Article 5 of the GDPR, but could also undermine the trust of individuals in the re-use mechanism, which is a fundamental aim of the Proposal (see recitals 14 and 19)[34].

75. In this regard, the EDPB and the EDPS recall that Article 6(4) GDPR clarifies the concept of 'compatible further processing' (of personal data). Indeed, according to the definition of 're-use' set out in Article 2(2) of the Proposal, when it concerns personal data, the re-use is to be regarded, under a data protection perspective, as a further processing of personal data held by public sector bodies for

[32] See EDPS Opinion on the European Strategy for Data, paragraph 10.
[33] See in this regard recital (52) of the Open Data Directive.
[34] See EDPS Opinion on the European Strategy for Data, paragraph 25.

subsequent not well described (commercial or non-commercial) purposes. However, Article 5 of the Proposal, concerning the conditions for re-use, does not provide any indication on the purposes for which the re-use may be lawfully authorised, nor it specifies that the purposes of any subsequent re-use have to be carefully identified and clearly defined in Union or Member State law in compliance with Article 6(1)(c) or 6(1)(e) and 6(3) of the GDPR[35], eventually satisfying the requirements of Article 23(1) of the GDPR pursuant to Article 6(4) of the GDPR[36].

76. More generally, the Proposal does not seem to lay down any legal obligation for public sector bodies to make data they held available for re-use, nor does it explicitly aim at safeguarding the objectives listed in Article 23 of the GDPR.

77. **Therefore, the EDPB and EDPS strongly recommend to amend the Proposal so as to clarify that the re-use of personal data held by public sector bodies may only be allowed if it is grounded in Union or Member State law which lays down a list of clear compatible purposes for which the further processing may be lawfully authorised or constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23 of the GDPR**.

78. **Furthermore and in line with the above recommendation, to allow a lawful access to personal data by "data users", as indicated by the definition of 'data users' pursuant to Article 2(6) of the Proposal, public sector bodies, which are competent under national or EU law to grant or refuse such access for the re-use, must rely on an adequate legal basis under Article 6 of the GDPR being applicable to the said disclosure. However, this aspect is not specified under Article 5 of the Proposal referring to the conditions for re-use of personal data held by public sector bodies.**

79. Indeed, recital 11 of the Proposal and the corresponding Article 5(3)-(6) does not refer to Union or Member State law that would provide the legal basis under Article 6(1)(c) or (e) of the GDPR, but lays down (bold added): *"In particular, personal data should only be transmitted for re-use to a third party where a legal basis allows such transmission*". In this respect, it shall be noted that the reference should be to the legal basis "under the GDPR". Moreover, the said recital restricts itself to state that "[*t]he public sector bodies, where relevant, should facilitate the re-use of data on the basis of consent of data subjects or permissions of legal persons on the re-use of data pertaining to them through adequate technical means. In this respect, the public sector body should support potential re-users in seeking such consent by establishing technical mechanisms that permit transmitting requests for*

[35] According to Article 6.3 GDPR, Union or Member State law under Article 6(1)(c) or 6(1)(e) of the GDPR should identify amongst other elements the "purpose limitation" of the personal data processing as well as the "purpose for which data may be disclosed".

[36] In another respect, the inclusion of data held by public sector bodies which are protected on grounds of statistical confidentiality in the scope of Chapter II of the Proposal, according to its Article 3(1)(b) and despite the principle stated in its Article 3(3), risks to contradict, the essential principles of data protection in the statistical sector and in particular, the purpose limitation principle, which strictly prohibits the use of confidential data for purposes that are not exclusively statistical, thus undermining trust of natural persons in providing their personal data for statistical purposes (see recital 27 of the above mentioned Regulation (EC) No 223/2009 on European statistics and Articles 4(1) and 4(2) of the Recommendation of the Council of Europe No R (97)18 concerning the protection of personal data collected and processed for statistical purposes).

consent from re-users, where practically feasible. No contact information should be given that allows re-users to contact data subjects or companies directly."

80. The wording of recital 14 of the Proposal is also unclear in setting out the interplay of this Chapter of the Proposal with the GDPR: *"[...] Additional safeguards should thus be put in place for situations in which the re-use of such public sector data is taking place on the basis of a processing of the data outside the public sector. Such an additional safeguard could be found in the requirement that public sector bodies should take fully into account the rights and interests of natural and legal persons (in particular the protection of personal data, commercially sensitive data and the protection of intellectual property rights) in case such data is transferred to third countries"*[37].

81. **Furthermore, the EDPB and the EDPS notice that Article 5(6) of the Proposal lays downs "Where the re-use of data cannot be granted in accordance with the obligations laid down in paragraphs 3 to 5 and there is no other legal basis for transmitting the data under Regulation (EU) 2016/679 [...]". In this regard, the EDPB and the EDPS are of the opinion that the conditions listed under paragraphs 3 to 5 (among which, access and re-use of data within a secure processing environment) cannot be considered as an alternative to the legal basis exhaustively listed under Article 6 of the GDPR, unless the reference to (Union or) Member State law is made in the aforesaid paragraphs[38].**

82. In addition, it is unclear the role of the public sector body in supporting re-users in obtaining the consent for the reuse by the data subject. As a further remark on Article 5(6) of the Proposal, the EDPB and the EDPS point out that this provision establishes an obligation for public sector bodies ("shall support"), whose content is not well defined. More to the point, the legal basis under the GDPR for contacting data subjects to collect their consent for the re-use should be specified, as well as the respective responsibility related to obtaining a valid consent under Article 7 of the GDPR.[39] In this regard, it should also be taken into account the clear imbalance of power which is often present in the relationship between the data subject and the public authorities[40]. In this context, in line with the GDPR accountability principle, the EDPB and the EDPS recall that the choice of an appropriate legal basis for the processing of personal data, as well as the demonstration that the chosen legal basis (in this case consent) can be validly applied, lies on the data controller.

83. **Therefore, in line with the principle of lawfulness established by the GDPR, the EDPB and EDPS strongly recommend to clarify, among the conditions for re-use provided for in Article 5 of the Proposal, that an appropriate legal ground under GDPR must be provided in Union or Member State law and carefully identified by public sector bodies with regard to any subsequent re-use of personal data.**

---

[37] In addition, the EDPB and EDPS note that public sector bodies should not just take into account but **comply with** the legal framework protecting the rights and interests of data subjects.
[38] It might also be worth specifying, for the sake of clarity, that intellectual property rights, referred to under Article 5(7), do not allow (constitute a legal basis for) the processing of personal data.
[39] Would it be the responsibility of the public sector body or of the re-user?
[40] In another respect, it should be reminded that consent in most cases is not an appropriate legal basis for the processing activities performed by public authorities. See the EDPB Guidelines 5/2020 on consent under Regulation 2016/579 at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

84. Other key elements to build the level of trust aimed at in the Proposal are the fairness and the transparency principles. According to these principles, individuals must be fully aware whether the personal data they provide to the public sector bodies, or that are further processed by the same bodies in the pursuit of their public tasks, will become subject to re-use and for which purposes, as well as the recipients or categories of recipients to whom the personal data will be disclosed taking into account that in most cases data subjects are compelled under national law to provide their personal data to public bodies because of legal obligations or because they apply for a public action or service[41].

85. However, among the conditions for re-use established in Article 5 of the Proposal, there is no reference to the obligations for the public sector bodies of informing the data subjects under the GDPR, nor to the need of involving them in the process of enabling the re-use of their personal data. This not only undermines the principles of fairness and transparency established by the GDPR to ensure that individuals have a clear overview and control on the possible uses of their own personal data, but also contradicts the same goals of the Proposal which is to increase trust of data subjects that the re-use "will take place in a manner that respects their right and interests" [42]. **Therefore, the EDPB and EDPS recommend to include in the Proposal an explicit reference to the obligations for the public sector bodies of informing the data subjects under the GDPR so that to foster the exercise of the rights conferred to them by the data protection legislation, especially the right to object pursuant to Article 21 of the GDPR. In this respect, the EDPB and EDPS also recommend to define in the Proposal adequate means by which individuals may participate, in an open and collaborative manner, in the process of allowing the re-use of their personal data.**

86. Moreover, to attain a reasonable level of trust in the re-use mechanism, public sector bodies, competent under national or EU law to allow access for the re-use must respect the principles of data minimisation and consider the special protection required for specific sectors routinely dealing with special categories of personal data, such as the health sector, when they establish the scope and conditions for allowing access for the re-use. In assuming these decisions, accuracy, storage limitation, integrity and confidentiality of personal data should also be carefully considered, as well as the potential impact on the concerned data subjects.

87. **In this regard, the EDPB and EDPS call the attention of the legislator to the need of addressing the necessary requirements of the protection of personal data, especially in "sensitive sectors" such as the health sector, when establishing the rules governing the re-use of personal data, as well as the related conditions and specific data protection safeguards.**

88. In particular, according to the GDPR, the data protection impact assessment (DPIA) is a key tool to ensure that data protection requirements are properly taken into account and the rights and interests of individuals are adequately protected, so as to foster their trust in the re-use mechanism. Therefore, the EDPB and EDPS recommend to include in the text of the Proposal that a DPIA must be performed by public sector bodies in case of data processing falling under Article 35 of the GDPR[43]. The DPIA will help to identify the risks and the appropriate data protection safeguards for the re-use addressing

[41] See Court of Justice of the European Union, C-201/14, *Smaranda Bara and Others*, 1 October 2015, ECLI:EU:C:2015:638.
[42] See Recital 14 of the Proposal
[43] See in this regard recital (53) of the Open Data Directive.

those risks, in particular for specific sectors routinely dealing with special categories of personal data. The decision on the re-use, in addition to being grounded on Union or Member State law, especially for some "sensitive sectors" (health sector, but also transport or energy grids) should be based on this assessment, as well as the specific conditions for the re-users and the concrete safeguards for data subjects(for example, clarifying the risks of re-identification of anonymised data and the safeguards against those risks). Finally, the results of such assessment, whenever possible, should be made public, as a further measure enhancing trust and transparency[44].

89. As for the conditions for re-use, Article 5(3) of the Proposal specifies that public sector bodies "may" impose an obligation to re-use only prior anonymized or pseudonymised personal data. This means that public sector bodies are not obliged to pre-process personal data so that to make available to re-users only prior anonymized or pseudonymised personal data. Consequently, public sector bodies may disclose to re-users even data which allow the natural persons - to whom the data relate - to be directly identified, if provision of anonymised data "would not respond to the needs of the re-user" [45]. In this case, on-premise or remote re-use of personal data within a secure processing environment could still be permitted by public sector bodies under Article 5(4) of the Proposal. However, given the rapid developments in re-identification techniques and the availability of advanced computational resources, the legislator should take into account that anonymisation, pseudonymisation, and even the use of secure environments cannot be considered in all cases as free from vulnerabilities, especially in the long term.

90. In this context, the EDPB and the EDPS welcome that recital 11 of the Proposal envisages that "the use of such secure processing environment" may be made by the public sector body *"conditional on the signature by the re-user of a confidentiality agreement that prohibits the disclosure of any information that jeopardises the rights and interests of third parties that the re-user may have acquired despite the safeguards put in place".* **However, the EDPB and the EDPS also recommend to include a reference to such confidentiality agreement in the legal text of the Proposal among the conditions for re-use laid down in Article 5. This agreement should also prohibit the re-users from re-identifying any individual to whom the data relates and should contain the obligation for the re-users to assess on an on-going basis the risks of re-identification and to report any data breach resulting in the re-identification of the individuals concerned not only to the Data Protection Authority and the data subjects pursuant to Articles 33 and 34 of the GDPR, but also to the public sector body concerned.**

91. **In any case, the EDPB and EDPS emphasize that anonymisation and pseudonymisation cannot be placed at the same level and should be weighted differently by public sector bodies in assessing the re-use from a data protection perspective. Indeed, anonymisation represents a means of fostering the public sector information re-use in a pro-competitive perspective, while also meeting the various requirements under data protection legislation, given that 'anonymous information', as defined in Recital 26 of the GDPR, does not fall within the scope of the said legislation. On the contrary, information which has undergone pseudonymisation (which could lead to re-identification by a natural person by the use of additional information) should still be considered "personal data", thus entailing the application of other measures required by the data protection legislation, while**

[44] See EDPS Opinion on the proposal for a recast of the Public Sector Information (PSI) re-use Directive, available at: https://edps.europa.eu/sites/edp/files/publication/18-07-11_psi_directive_opinion_en.pdf
[45] See recital 11 of the Proposal

reducing the risks for data subjects and helping public sector bodies and re-users to meet data protection obligations (in particular the principles of data protection by design and by default and data minimisation). The latter considerations apply also to the measures envisaged by Article 5(4) of the Proposal that public sector bodies may impose as conditions for re-use.

3.3.3 Article 5(11): re-use of "highly sensitive" non-personal data

92. Article 5(11) introduces the concept of non-personal data that have been identified as "highly sensitive", as regards the transfer to third countries, by Union law. Recital 19 of the Proposal provides some examples: "in the health domain, certain datasets held by actors in the public health system, such as public hospitals" "identified as highly sensitive health data", "for example in the context of the European Health Data Space or other sectoral legislation". With regard to such non-personal data, the Commission shall adopt delegated acts laying down special conditions applicable to the transfer of such data to third countries.

93. In this regard, the EDPB and the EDPS note that even if information in a anonymised data set does not present a risk of directly identifying or singling out a natural person, when this information is combined with other available information, it could entail the risk of indirect identification, so that it is likely to fall within the scope of the definition of personal data. Indeed, the more information is available and data are re-used and shared, the more difficult it will be to ensure anonymisation over time.[46] Consequently, the EDPS and the EDPB would like to draw attention to the fact that much of the data already today -and increasingly in the future- generated and processed by techniques of artificial intelligence, machine learning, internet of things, cloud computing and big data analysis, are often likely to fall within the scope of the definition of personal data. In this scenario, **the EDPB and the EDPS calls upon the legislator to consider that even the re-use of non-personal "highly sensitive" data envisaged by the Proposal may have an impact on the protection of personal data, especially if such non-personal data are the result of the anonymisation of personal data and thus information originally related to individuals.** Indeed also in these cases, the data subjects' fundamental rights to privacy and data protection must be fully ensured. Moreover, the EDPB and the EDPS strongly recommend clarifying the concept of "highly sensitive non-personal data", as a minimum by providing concrete examples.

3.3.4 Article 6: fees for data re-use

94. As for the fees envisaged under Article 6 of the Proposal, the EDPB and the EDPS note that the Open Data Directive contains an explicit reference to 'anonymisation costs' in Recitals 36 and 38 as well as in Article 6, paragraphs (1), (4) and (5). In particular, the Open Data Directive provides for an exception to the re-use of documents free of charge in order to allow public sector bodies to charge re-users the reasonable expenses they incur in to pre-process, aggregate and/or anonymise the personal data

[46] See in this regard, the WP29 Opinion 05/2014 on Anonymisation techniques (WP 216) as well as the Judgment of the ECJ of 19 October 2016, Patrick Breyer v Bundesrepublik Deutschland, in case C-582/14 which refers to Recital 26 of Directive 95/46/EC, looking at the legal and practical means by which re-identification may be affected by the use of additional data in the hands of third parties. The forthcoming EDPB guidelines on anonymisation/pseudonymisation will further elaborate upon this matter.

offered for re-use, in situations where the use of such techniques would be justified in light of the increased risks deriving from offering such data for re-use.

95. Given that, in certain cases, the pseudonymisation or anonymisation of information held by public sector bodies can be a complex, time-consuming and expensive task requiring expertise that might not always be available, the EDPB and the EDPS recommend including in Article 6(5) of the Proposal that **fees charged by public sector bodies for allowing the re-use of data may duly take into account the costs incurred by public sector bodies for the pseudonymisation or anonymisation** of personal data made available for reuse.

96. It can also be noted that **the Proposal reverses the general principle established by the Open Data Directive of "free of charge" re-use.** Indeed, Article 6(1) of the Proposal states that *"public sector bodies which allow re-use of the categories of data referred to in Article 3 (1) may charge fees for allowing the re-use of such data."* In this regard, the interplay with the Open Data Directive is therefore unclear.

97. Moreover, it can be observed that, even though Article 6(5) specifies that "Fees shall be derived from the costs related to the processing of the requests for re-use (...)", the Proposal seems to introduce financial incentives to public sector bodies to allow the re-use of personal data.

98. It also has to be noted thatArticle 6(4) imposes an obligation to public sector bodies to "*take measures to incentivize the reuse of the categories of data referred to in Article 3 (1) [which include personal data] for non-commercial purposes and by small and medium-sized enterprises in line with State aid rules*."

99. This aspect, also in the light of the criticalities of the Proposal described in the general comments of this Joint Opinion, is problematic from a data protection viewpoint, under both legal and practical implementation's perspective. In particular, the lack of clarity on the type of incentives and addressees thereof may raise additional questions as to whether consent, as one of the legal basis relied upon under Article 5(6) of the Proposal for the re-use personal data, will be the appropriate legal ground, especially with regard to the individuals' freedom of choice to refuse to provide their consent to the re-use of their personal data or to withdraw it[47].

3.3.5 Governance and institutional aspects: Article 7 (competent bodies). Article 8 (single information point).

100. The Proposal provides that Members States will have to set up a single contact point for reuse of public sector data (Article 8), and to establish bodies in charge of supporting public sector bodies with technical means and legal assistance for reuse of public sector data (Article 7). Pursuant to Article 7(3), such "competent bodies" may be entrusted to grant access for the reuse of data, including personal data.

[47] As stated in the EDPB Guidelines 05/2020 on consent under GDPR, in general terms, any element of inappropriate pressure or influence upon the data subject (which may be manifested in many different ways) which prevents a data subject from exercising their free will, shall render the consent invalid.

101. Therefore, with regard to the competent bodies, they will, inter alia, assist the public sector bodies in obtaining consent or permission for the re-use and can also be entrusted to grant access for the re-use of data held by the public sector body, including personal data.

102. Firstly, the provision under Article 7(2)(c) should be clarified, due in particular to the vagueness of the terminology used ("permission by re-users for reuse"; "altruistic and other purposes"; "in line with specific decisions of data holders"). The overall meaning of the provision ("the competent bodies assist the public sector bodies, where relevant, in obtaining consent or permission *by re-users for re-use* for altruistic and other purposes in line with specific decisions of data holders") is therefore also unclear.

103. Secondly, despite those bodies are essentially tasked with support and advisory duties vis-à-vis public sector bodies for data re-use, some of their tasks deal with implementing the safeguards set out in the data protection legislation and fostering the protection of the rights and interests of individuals with regards to their personal data. However, Chapter II of the Proposal does not clarify whether data protection supervisory authorities - to which the GDPR also confers, among others, advisory powers - may be designated as the competent body under Article 7 of the Proposal[48].

104. In this regard, the EDPS and the EDPB firstly underline that the designation and multiplication of competent bodies that may deal, to some extent, with personal data processing under Chapter II of the Proposal could lead to real complexity for public sector bodies, re-users and data subjects, and also affect consistency in terms of monitoring the application of the provisions of the GDPR. **Hence, inasmuch as personal data is being subject to re-use on the basis of the Proposal, the EDPB and the EDPS consider that the data protection supervisory authorities should be the only ones competent for the oversight of such personal data processing. Adequate resources should be provided to these authorities to allow them to effectively and efficiently perform this task.**

105. **Furthermore, should specific bodies be designated to assist public sector bodies and data re-users and be entrusted to grant access for the reuse of data, including personal data, such bodies may not be referred as "competent" as they would not act as a supervisory authority able to monitor and enforce the provisions related to the processing of personal data. In order to ensure legal certainty and consistency of the application of the EU acquis in the field of personal data protection, the activities and obligations of such designated bodies shall also be subject to the direct competence and supervision of data protection authorities, when personal data is involved.**

106. **As per their competence and tasks under the GDPR, data protection authorities have already specific expertise in the monitoring of the compliance of data processing, as well as in promoting awareness of controller and processor of their obligation related to the processing of personal data. Therefore, in order to ensure consistency between the institutional framework envisaged by Chapter II of the Proposal and the GDPR, the EDPB and the EDPS recommend to clarify that the main competent authorities for the supervision and enforcement of the provisions of Chapter II related to the processing of personal are the data protection supervisory authorities. The latter authorities should**

[48] As it is the case, for example, in the context of existing data spaces, such as the French Health Data Hub, where the FR data protection authority is the one competent to authorise access to specific personal data. See also in this regard the advisory powers conferred to the data protection authorities in the context of a DPIA, in order ensure their compliance with the rules for the protection of personal data according to Articles 57(1)(l) and 58(3)(a) of the GDPR.

work closely with the specific bodies designated, under the Proposal, to assist public sector bodies and re-users and entrusted to grant access for the reuse of data, in consultation with other relevant sectorial authorities, when necessary, so as to ensure a coherent application of these provisions.

107. The EDPB and the EDPS also observe that the Proposal does envisage under Article 8(4) a mechanism for redress for re-users where they wish to challenge the decision of refusing access for re-use that is different from the one established under the Open Data Directive. Under the Open Data Directive (See Article 4(4)), in particular, the means of redress shall include the possibility of review by an impartial review body with the appropriate expertise, such as, among others, *"the supervisory authority established in accordance with Regulation (EU) 2016/679 or a national judicial authority, whose decisions are binding upon the public sector body concerned"*. In this respect, without prejudice to the observations already made in this Joint Opinion on the need of clarifying the interplay of the Proposal with the Open Data Directive, the EDPB and the EDPS call the attention of the legislator on the inconsistencies between those two set of rules.

3.4 Requirements applicable to data sharing service providers

The Explanatory Memorandum illustrates that "*Chapter III aims to increase trust in sharing personal and non-personal data and lower transaction costs linked to B2B and C2B data sharing by creating a notification regime for data sharing providers. These providers will have to comply with a number of requirements, in particular the requirement to remain neutral as regards the data exchanged. They cannot use such data for other purposes. In the case of providers of data sharing services offering services for natural persons, the additional criterion of assuming fiduciary duties towards the individuals using them will also have to be met. The approach is designed to ensure that data sharing services function in an open and collaborative manner, while empowering natural and legal persons by giving them a better overview of and control over their data. A competent authority designated by the Member States will be responsible for monitoring compliance with the requirements attached to the provision of such services*."[49]

108. Article 9(1) of the Proposal, specified under recital 22, sets out three different types of data sharing services:

- under letter (a), intermediary between data holders which are legal persons and potential data users;

- under letter (b), intermediation services between data subjects and potential data users;

- under letter (c), 'data cooperatives'.

109. Having regard to the first type of data sharing service, Article 9(1)(a) refers to "*intermediation services between data holders which are legal persons and potential data users, including making available the technical or other means to enable such services; those services may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or joint exploitation of data, as well as the establishment of a specific infrastructure for the interconnection of data holders and data users.*"

[49] Explanatory Memorandum, page 7.

110. Recital (22) specifies: "*Providers of data sharing services (data intermediaries) are expected to play a key role in the data economy, as a tool to facilitate the aggregation and exchange of substantial amounts of relevant data. Data intermediaries offering services that connect the different actors have the potential to contribute to the efficient pooling of data as well as to the facilitation of bilateral data sharing. Specialised data intermediaries that are independent from both data holders and data users can have a facilitating role in the emergence of new data-driven ecosystems independent from any player with a significant degree of market power. This Regulation should only cover providers of data sharing services that have as a main objective the establishment of a business, a legal and potentially also technical relation between data holders, including data subjects, on the one hand, and potential users on the other hand, and assist both parties in a transaction of data assets between the two. It should only cover services aiming at intermediating between an indefinite number of data holders and data users, excluding data sharing services that are meant to be used by a closed group of data holders and users.*"

111. **In light of the above, the EDPB and the EDPS consider that the issue referred to under the general remarks of this Joint Opinion as overarching concern, namely the risk that the Proposal creates a parallel set of rules, which are not consistent with the GDPR, is particularly evident with reference to Chapter III of the Proposal. Indeed, it is unclear the interplay of the provisions under Article 9 of the Proposal, referring to 'data holders', 'potential data users', 'the exchange or joint exploitation of data', 'the interconnection of data holders and data users', with the rules and principles of the GDPR.**

112. We recall that the data sharing service as platform "intermediating between an indefinite number of data holders and data users" excluding the use by a closed group of data users, in so far as the intermediation relates to personal data, shall be compliant in particular with the principle of data protection by design and by default under Article 25 of the GDPR[50].

---

[50] See Article 25(2): "The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data **are not made accessible without the individual's intervention to an indefinite number of natural persons**."
See also EDPB Guidelines 4/2019 on the principle of privacy by design and by default, at page 20:
"Key design and default purpose limitation elements may include:
- Predetermination – The legitimate purposes shall be determined before the design of the processing.
- Specificity – The purposes shall be specified and explicit as to why personal data is being processed.
- Purpose orientation – The purpose of processing should guide the design of the processing and set processing boundaries.
- Necessity – The purpose determines what personal data is necessary for the processing.
- Compatibility – Any new purpose must be compatible with the original purpose for which the data was collected and guide relevant changes in design.
- Limit further processing – The controller should not connect datasets or perform any further processing for new incompatible purposes.
- Limitations of reuse – The controller should use technical measures, including hashing and encryption, to limit the possibility of repurposing personal data. The controller should also have organisational measures, such as policies and contractual obligations, which limit reuse of personal data.

113. The EDPB and the EDPS also point out to the data protection principles of transparency (and purpose limitation) of the processing of personal data. As stated in the WP29 Guidelines on transparency "*the data subject should ... be able to determine in advance what the scope and consequences of the processing entails*" (...) "*namely the kind of effect will the specific processing described in a privacy statement/notice actually have on a data subject*".[51]

114. **The concept of data sharing service as platform "intermediating between an indefinite number of data holders and data users", as kind of open data marketplace, would be contrary to the aforesaid data protection principles of privacy by design and by default, transparency and purpose limitation <u>if the platform does not allow a pre-selection of and prior information about the purposes and users of her or his personal data by and to the data subject</u>. For the sake of clarity, the Proposal should specify, at least in a recital, this aspect.**

115. **The scope of the notion of data intermediary between data holders and legal persons is also unclear, and hence should be better specified**[52].

116. As a general observation, it can also be remarked that the Proposal does not specify **how (according to which GDPR legal basis) data sharing service providers will collect personal data for the sharing purposes.**

117. It is also unclear **whether data sharing service providers can intermediate data allowed for re-use by public sector bodies** under Chapter II of the Proposal.

118. It is also key, for transparency reasons and to increase (rather than decrease) the level of citizens' trust, to make clear in the Proposal that the data sharing service will be provided upon payment of a

---

- Review – The controller should regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation."

[51] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 WP260, rev.01, page 7.

[52] Recital 22 specifies: "[..] Providers of **cloud services** should be excluded, as well as **service providers that obtain data from data holders, aggregate, enrich or transform the data and licence the use** of the resulting data to data users, without establishing a direct relationship between data holders and data users, for example **advertisement or data brokers, data consultancies, providers of data products resulting from value added** to the data by the service provider. At the same time, data sharing service providers should be allowed to make **adaptations to the data exchanged, to the extent that this improves the usability** of the data by the data user, where the data user desires this, such as to convert it into specific formats. In addition, **services that focus on the intermediation of content, in particular on copyright-protected content, should not be covered** by this Regulation.

Data exchange platforms that are exclusively used by one data holder in order to enable the use of data they hold as well as platforms developed in the context of objects and devices connected to the Internet-of-Things that have as their main objective to ensure functionalities of the connected object or device and allow value added services, should not be covered by this Regulation. 'Consolidated tape providers' in the sense of Article 4 (1) point 53 of Directive 2014/65/EU of the European Parliament and of the Council as well as 'account information service providers' in the sense of Article 4 point 19 of Directive (EU) 2015/2366 of the European Parliament and of the Council should not be considered as data sharing service providers for the purposes of this Regulation. Entities which restrict their activities to facilitating use of data made available on the basis of data altruism and that operate on a not-for-profit basis should not be covered by Chapter III of this Regulation, as this activity serves objectives of general interest by increasing the volume of data available for such purposes."

'price' by data holders and data users. This aspect can be deducted from the wording of Article 11(3) of the Proposal[53], but is unclear and incomplete (it does not provide a clear picture of the monetary transactions accompanying the processing of personal data). The clear incentive to 'monetize' personal data also increases the importance of checks on data protection compliance[54]. Regrettably, in this regard, as well as in relation to the other chapters of the Proposal, the impact assessment[55] does not take the data protection risks into account.

119. Moreover, the EDPB and the EDPS observe that the Proposal does not provide a clear picture, for instance via examples in the recitals, of the 'use cases' of data sharing services (whose 'monetary transaction aspect', as highlighted, shall be made clear to the public and to the persons concerned when this is the case). For instance, recital (22) specifies what is not a data exchange platform to be considered 'data intermediary': "*Data exchange platforms that are exclusively used by one data holder in order to enable the use of data they hold as well as platforms developed in the context of objects and devices connected to the Internet-of-Things that have as their main objective to ensure functionalities of the connected object or device and allow value added services, should not be covered by this Regulation*", but does not provide in this regard the envisaged use case.

3.4.1 Data intermediaries under Article 9(1) (b): intermediation services between data subjects and potential data users[56].

120. The EDPB and the EDPS note that the provisions related to intermediation services between data subjects that seek to make their personal data available and potential data users in the exercise of the rights provided in Regulation (EU) 2016/679, as per article 9(1)(b), is to be applied without prejudice to the effective application of the data subjects' rights and data controller's obligations as per the GDPR.

121. The Proposal however does not specify the modalities upon which such service providers would effectively assist individuals in exercising their rights under the GDPR nor provides indication as to which personal data processing such assistance would apply and towards which data users precisely[57].

122. The EDPB and the EDPS first of all consider that the effective exercise of data subjects' rights and the possible modalities for such exercise are provided for by the GDPR, under the monitoring of national supervisory authorities as per Article 51 of that same Regulation. The lack of clarity on the precise

[53] Article 11(3) of the Proposal lays down: "the provider shall ensure that the procedure for access to its service is fair, transparent and non-discriminatory for both data holders and data users, including as regards **prices**."
[54] In this regard, the EDPB is developing guidance on the collection and use of personal data against financial remuneration.
[55] Impact Assessment accompanying the Data Governance Act, SWD(2020) 295 final, available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2020:0295:FIN:EN:PDF
[56] Article 9(1)(b) of the Proposal refers to: "intermediation services between data subjects that seek to make their personal data available and potential data users, including making available the technical or other means to enable such services, in the exercise of the rights provided in Regulation (EU) 2016/679."
[57] Article 11(10) of the Proposal is still quite vague in its wording "the provider offering services to data subjects **shall act in the data subjects' best interest when facilitating the exercise of their rights**, in particular by advising data subjects on potential data uses and standard terms and conditions attached to such uses;"

modalities in the assistance provided for the exercise of data subjects' rights, as well as on the recipients of such process and their obligations towards data subjects may lead to further legal uncertainties in effectively exercising data subjects' rights as per the GDPR.

123. **The EDPB and the EDPS would therefore recommend that the Proposal reflects the EU legal framework (GDPR) according to which such modalities, as well as related obligations applicable to data sharing services providers and recipients, can be further specified by the European Data Protection Board, in accordance with Article 70 of the GDPR[58].**

124. It is also unclear whether the intermediation services under letter (b) of Article 9(1) of the Proposal, for which a definition is not provided under its Article 2, refer to and refer only to (and to which extent) Personal Information Management Systems (PIMS). The EDPB and the EDPS point out to the difference between PIMS, allowing management of personal data and facilitating the exercise of data subjects' rights ('interfacing with the data subject')[59], on the one hand, and business to business data sharing service providers (whose correlation with 'data brokers' is unclear), on the other hand. It is in relation to the latter, where the data subject is more far-way and at risk of not having a clear overview and control over the sharing of his or her personal data, that criticalities under the data protection viewpoint may be higher[60].

125. However, in all cases transparency, fairness and purpose limitation principles shall apply.

126. In its Opinion on PIMS, the EDPS pointed out that *"In any event, it is crucial to ensure the transparency of the business model vis-à-vis the individuals whose data are being processed so that they are aware of the interests at stake (of PIMS and other service providers) and can use PIMS in full awareness"* [61].

---

[58] In this regard, the EDPB is currently working on guidelines on data subject rights.

[59] See the EDPS Opinion on Personal Information Management Systems, 20 October 2016, available at: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf

[60] See EDPS Opinion on the European Strategy for Data, paragraph 20: "At the same time, the EDPS underlines the need of caution with regard to the role of data brokers that are actively engaged in the collection of huge datasets, including personal data from different sources. They tap into a variety of data sources used for data-related services, such as data that are disclosed for other unrelated purposes; data from public registers (open data), as well as data "crawled" from the Internet and social media, often in violation of data protection legislation. In this context, the EDPS notes that the activities of big data brokers are under increased scrutiny and are investigated by a number of national data protection authorities."

[61] See page 13, para. 52, of the EDPS Opinion on Personal Information Management Systems, 20 October 2016, available at: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf
See also para 53, page 13: "*The model of PIMS seems to invite a debate over who 'owns' our personal data. Individuals in the EU have a fundamental right to the protection of their personal data, based upon Article 8 of the EU Charter of Fundamental Rights. Detailed rights and obligations relating to the exercise of this right are regulated in further detail in the recently adopted GDPR. These issues are not specific to PIMS: personal data is often perceived as the 'currency' we pay for so-called 'free' services on the internet. This trend does not, however, mean that personal data of individuals can legally be considered as property which can be traded freely as any other property on the market. On the contrary, as a matter of principle PIMS will not be in a position to 'sell' personal data, but rather, their role will be to allow third parties to use personal data, for* ***specific purposes****, and* ***specifics periods of time****, subject to* ***terms and conditions identified by the individuals themselves****, and* ***all other safeguards provided by applicable data protection law***."

127. The Proposal provides some clarifications related to providers of data sharing services not established in the Union in order to determine whether such a provider is offering services within the Union. This specification, under recital 27 of the Proposal, seems in line with recital (23) of the GDPR. It might be useful, for the sake of legal certainty, specifying that, in case of processing of personal data, the aforesaid data sharing service providers not established in the Union are subject to the rules and principles of the GDPR.

3.4.2 Data intermediaries under Article 9(1) (c): 'data cooperatives'

128. The EDPB and the EDPS underline that the notion of "service of data cooperatives", introduced in Article 9(1)(c) of the Proposal[62], remains unclear both in terms of nature and obligations. In this regard, a clear definition of such data sharing services providers, as well as their applicable obligations, should be introduced in order to avoid any legal uncertainty in the provision of such services.

129. While the Proposal specifies that data cooperatives "*seek to strengthen the position of individuals in making informed choices before consenting to data use, influencing the terms and conditions of data user organisations attached to data use or potentially solving disputes between members of a group on how data can be used when such data pertain to several data subjects within that group*"[63], it is to be recalled that transparency obligations, as well as the conditions for the valid consent of the data subject as per Article 6(1)(a) of Regulation (EU) 2016/679 and the condition for the processing of personal data under this legal basis, are defined and provided for by that same regulation.

130. **The EDPB and the EDPS therefore consider that the position of individuals in making informed choice, or the solving of potential dispute on how data can be used, are not to be considered as negotiable conditions but rather as data controllers' obligations as per Regulation (EU) 2016/679. In this regard, it is also to be pointed out that the reference in Recital (24) of the Proposal to data that would "pertain" to several data subject, insofar as it relates to personal data, may not be consistent with the definition of personal data as per Regulation (EU) 2016/679[64], which refers to "any information relating to an identified or identifiable natural person".**

131. Furthermore, as recalled in Recital (24) of the Proposal, "*the rights under Regulation (EU) 2016/679 can only be exercised by each individual and cannot be conferred or delegated to a data cooperative*". The EDPB and the EDPS consider that the articulation of such principles with the possibility for data cooperatives to be conferred powers to "negotiate terms and conditions for data processing before they consent" is unclear at least, if not directly contradictory. Indeed, the "terms and conditions" for the processing of personal data are - as a matter of fact - those enshrined in the GDPR and, therefore, they cannot be amended or superseded by means of a contract or other type of private arrangements.

---

[62] Article 9(1)(c) of the Proposal refers to "services of data cooperatives, that is to say services supporting data subjects or one-person companies or micro, small and medium-sized enterprises, who are members of the cooperative or **who confer the power to the cooperative to negotiate terms and conditions for data processing before they consent**, in **making informed choices before consenting to data processing**, and **allowing for mechanisms to exchange views on data processing purposes and conditions that would best represent the interests of data subjects or legal persons**."

[63] Recital (24) of the Proposal.

[64] Definition under Article 4(1) of the GDPR.

3.4.3 Article 10: notification regime - general requirements to be eligible for registration - content of the notification; outcome (and timing) of the notification. Article 11: conditions for providing data sharing services

132. Chapter III of the Proposal establishes an obligation for providers of data sharing services as described under Article 9(1) to submit a notification to the competent authority (mandatory notification). Article 10(1) and (2) provide rules on the identification of the jurisdiction of the Member State for the purposes of the Proposal. This is the jurisdiction of the Member State of the main establishment of the data sharing service provider or the Member State of establishment of the legal representative of the data sharing service provider not established in the Union.

133. The information to be included in the notification is provided under Article 10(6), letters (a)-(h) of the Proposal[65]. In addition, Article 10(7) lays down that "*At the request of the provider, the competent authority shall, within one week, issue a standardised declaration, confirming that the provider has submitted the notification referred to in paragraph 4.*"

134. The notification regime, as highlighted in the Explanatory Memorandum, "consists of a *notification obligation with ex post monitoring of compliance with the requirements to exercise the activities by the competent authorities of the Member States*"[66]. This aspect is further specified under recitals (30) and (31) of the Proposal[67].

135. Hence, the 'vetting' of the data sharing service provider is limited to the verification by the competent authority of the (mainly formal) requirements set out in Article 10 and shall occur within a very short time-limit (one week from the date of notification).

---

[65] "The notification shall include the following information:
(a) the name of the provider of data sharing services;
(b) the provider's legal status, form and registration number, where the provider is registered in trade or in another similar public register;
(c) the address of the provider's main establishment in the Union, if any, and, where applicable, any secondary branch in another Member State or that of the legal representative designated pursuant to paragraph 3;
(d) a website where information on the provider and the activities can be found, where applicable;
(e) the provider's contact persons and contact details;
(f) a description of the service the provider intends to provide;
(g) the estimated date for starting the activity;
(h) the Member States where the provider intends to provide services."

[66] Explanatory Memorandum, page 5.

[67] "(30) A notification procedure for data sharing services should be established in order to ensure a data governance within the Union based on trustworthy exchange of data. The benefits of a trustworthy environment would be best achieved by imposing a number of requirements for the provision of data sharing services, but **without requiring any explicit decision or administrative act by the competent authority for the provision of such services**.
(31) In order to support effective cross-border provision of services, the data sharing provider should be requested to **send a notification only to the designated competent authority from the Member State where its main establishment is located or where its legal representative is located**. Such a **notification should not entail more than a mere declaration of the intention to provide such services and should be completed only by the information set out in this Regulation**." (emphasis added)

136. **In this regard, the EDPB and the EDPS note that the 'vetting' regime is almost 'declarative' and that the Commission has opted for the most 'loose' regime (as opposed for instance to an authorization regime). The EDPB and the EDPS observe that, at least with regard to the processing of personal data, the regime should be more protective (that is, provide more checks and safeguards for the data subjects, including on the crucially important data protection aspects). This would also allow ensuring the higher level of trust aimed at by the Commission.**

137. **In order to address this concern, in particular Recital 31 of the Proposal should be amended.**

138. According to the data protection principle of accountability, data sharing service providers shall be able among others to demonstrate that they put in place policies and procedures that allow data subjects to easily exercise their individual data protection rights (procedures for ensuring compliance with data subjects' rights), and should document the decisions about the data sharing (including in particular the purposes for which the personal data will be shared and the recipients or categories of recipients to whom they will be disclosed), evidencing their compliance with data protection law[68]. These aspects (which should form the 'core' of the labelling envisaged by the Proposal[69]) will have the effect of creating greater trust in data sharing service providers by the public.

139. The EDPB and the EDPS also remark that the provisions of data sharing services, as laid down under Article 11, shall be subject to conditions under (1)-(11). In this regard, the EDPB and the EDPS notice that while reference is made among the conditions to compliance with competition rules (under (9)), these (exhaustively listed) conditions do not include compliance with data protection rules.

140. **In light of the elements above, and considering the possible risk for data subject in the personal data processing that may be undertaken by data sharing service providers, the EDPB and the EDPS consider that the declaratory notification regime as laid down in the Proposal does not provide for a sufficiently stringent vetting procedure applicable to such services. The EDPB and the EDPS recommend exploring alternative procedures which should notably take into account a more systematic inclusion of accountability and compliance tools for the processing of personal data as per the GDPR, in particular the adherence to a code of conduct or certification mechanism.**

---

[68] According to Article 30 of the GDPR: "Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1). [...]"

[69] The Impact Assessment of the Proposal refers to labelling or certification, among others, at page 19 "Mutual recognition of certification/labelling mechanisms and of a trust scheme for data altruism will make it possible to collect and use the data at the necessary scale."; page 25 "certification/labelling framework for data intermediaries"; page 26: "A certification or labelling framework would allow novel data intermediaries to increase their visibility as trustworthy organisers/orchestrators of data sharing or pooling."

141. It can also be observed that the safeguards provided in Chapter IV of the Proposal for data altruism organizations (Article 18, transparency requirements; Article 19, specific requirements) are not foreseen by the Proposal having regard to data sharing service providers, despite the possible impact also of these data sharing services on the rights and freedoms of the persons concerned.

142. This difference between the two notification regimes might give raise to interpretation *a contrario* that the requirements established for data altruism organizations and relating to the protection of personal data insofar as personal data are processed (for instance, informing data holders about any processing outside the Union[70]) do not apply to data sharing service providers.

143. **In this regard, the EDPB and the EDPS notice in particular that organisations involved in 'data pooling' or data sharing arrangements should adhere to certain common standards, whose supervision by independent data protection authorities shall be expressly recalled by the Proposal, related not only to the conditions for interoperability, but also to the conditions for ensuring the lawfulness of the processing of personal data and facilitating the exercise of data subject rights (e.g., through joint controllers' arrangements pursuant to Article 26 of the GDPR).**

144. Moreover, the EDPB and the EDPS notice that the Proposal refers to scenarios (use of metadata for the development of the data sharing service, under Article 11(2); continued access by data holders and data users after insolvency of the data sharing provider to data stored by the latter, under Article 11(6)) which need specifications in order to bring them in line with rules and principles on the protection of personal data.

145. The EDPB and the EDPS also remark that the comments made under the general remarks of this opinion, related to the definitions used in the Proposal and to the issue of the legal basis under the GDPR for the processing of personal data, are also relevant having regard to the provisions of Chapter III of the Proposal.

146. Furthermore, with particular reference to the aim of ensuring better control on the access and use of personal data by the data subject, we recall that the principle of purpose limitation is of special importance having regard to business-to-business data intermediaries. Recital (26) of the Proposal[71], which seems to identify the purpose of the processing of personal data with the intermediation in the sharing of data, without further specifications, might raise concerns from a data protection viewpoint[72].

---

[70] Article 19(1)(b) of the Proposal.

[71] Recital (26) of the Proposal: "A key element to bring trust and more control for data holder and data users in data sharing services is the neutrality of data sharing service providers as regards the data exchanged between data holders and data users. It is therefore necessary that data sharing service providers **act only as intermediaries** in the transactions, and do not use the data exchanged for **any other purpose**. [..]"

[72] See also Article 2(4) of the Proposal: 'metadata' means data collected on any activity of a natural or legal person **for the purposes of the provision of a data sharing service";** Article 2(7): "'data sharing' means the provision by a data holder of data to a data user for **the purpose of joint or individual use of the shared data**"; Article 11(1): the provider may not use the data for which it provides services for **other purposes than to put them at the disposal of data users.**"

147. The EDPB and the EDPS consider that the remarks made under Section 3.3 of this Joint Opinion concerning the reuse of personal data held by public sector bodies are also relevant having regard to data sharing services:

- any sharing or access to personal data must be strictly defined in scope and purpose and must occur in full compliance with the GDPR, taking into account the requirements of lawfulness, purpose limitation and the legitimate expectations of the data subjects;

- it should be clear that each 'actor' of the data processing chain, including the data sharing service provider and the user(s), shall provide the data subjects with the information under Article 13 and 14 of the GDPR (oftentimes, Article 14, applicable where personal data have not been obtained by the data subject, will be the relevant provision of the GDPR in this context). We recommend adding in this regard that the data sharing service provider shall provide the data subject with user-friendly tools showing him/her a comprehensive view of how his/her personal data are shared, as well as a user-friendly tool to withdraw consent in case the service provided consists of a tool for obtaining consent from data subjects with regard to the processing of their personal data under Article 11(11) of the Proposal

- the data protection impact assessment (DPIA) is a key tool to ensure that data protection requirements are properly taken into account and the rights and interests of individuals are adequately protected, so as to foster their trust in the re-use mechanism. Therefore, the EDPB and EDPS recommends to include in the text of the Proposal that **a DPIA must be performed by data sharing service providers (and by the data user) in case of data processing falling under Article 35 of the GDPR**. Indeed, the data sharing envisaged under the Proposal may involve large-scale processing, which combines data from a variety of sources, potentially involving special categories of data and/or personal data of vulnerable groups of data subjects. In this case, data controllers have the obligation to perform a DPIA in accordance with Article 35 of the GDPR. Moreover, whenever possible, the results of such assessments, as a trust and transparency-enhancing measure, shall be made public by the data sharing service provider as well as by the user(s).

3.4.4 Articles 12 and 13: competent authorities and monitoring of compliance (with Articles 10 and 11).

148. Article 12(3) of the Proposal provides that "*The designated competent authorities, the data protection authorities, the national competition authorities, the authorities in charge of cybersecurity, and other relevant sectorial authorities shall exchange the information which is necessary for the exercise of their tasks in relation to data sharing providers.*"

149. This wording provides for an even minor role for data protection authorities than the wording used by the Proposal in relation to data altruism organisations[73], which refers to "*cooperation with data protection authorities*".

[73] Article 20(3): "The competent authority shall undertake its tasks [of authority responsible for the register of recognised **data altruism organizations** and for the monitoring of compliance with the requirements of Chapter

150. In this regard, as highlighted in Section 3.7 of this Joint Opinion, the EDPB and the EDPS recall that many provisions of this Chapter as well as of the other Chapters of the Proposal relate to the processing of personal data and that the data protection authorities are the authorities 'constitutionally' competent for the supervision related to the protection of personal data pursuant to Article 8 of the Charter and Article 16 TFEU.

151. Having regard to Article 13 of the Proposal, monitoring of compliance, notwithstanding recital (28) which states that the Proposal should be without prejudice to the responsibility of supervisory authorities to ensure compliance with the GDPR, the EDPB and the EDPS consider that the governance and monitoring of compliance should be better defined in order to ensure a more appropriate vetting of data sharing service providers (and data altruism organisations) including on compliance with the GDPR; and to avoid, at the same time, any overlap or conflict of attribution between the authorities established under the Proposal (which, according to the wording of Articles 12(3) -and 20(3)-, are not data protection authorities) and the data protection authorities.

152. **The EDPB and EDPS therefore consider that such better definition of governance would be provided by the designation of data protection authorities as the main competent authorities to monitor and supervise compliance with the provisions of Chapter III of the Proposal.**

153. The designation of data protection authorities as the main competent authorities for the supervision and enforcement of the provisions under Chapter III of the Proposal would also ensure a more consistent regulatory approach across Member State and therefore contribute to the consistent application of the Proposal. As per their competence and tasks under the GDPR, data protection authorities have already specific expertise in the monitoring of the compliance of data processing, the auditing of specific data processing activities and data sharing, the assessment of the adequate measures to ensure a high level of security for the storage and transmission of personal data, as well as in promoting awareness among controllers and processors of their obligation related to the processing of personal data.

154. The designation of data protection authorities as main competent authority for the supervision and enforcement of the provisions under Chapter III shall be supported with the foreseen provision under Article 12(3) allowing for the exchange of information between the data protection authorities, the national competition authorities, the authorities in charge of cybersecurity, and other relevant sectorial authorities in order to ensure a coherent application of these provisions.

IV of the Proposal] **in cooperation with the data protection authority**, where such tasks are related to processing of personal data, and with relevant sectoral bodies of the same Member State. For any **question requiring an assessment of compliance with Regulation (EU) 2016/679**, the competent authority shall first seek an opinion or decision by the competent supervisory authority established pursuant to that Regulation and comply with that opinion or decision."
It also has to be noted that recital 28 -having regard to **providers of data sharing services**- specifies that "this Regulation should be **without prejudice to** the obligation of providers of data sharing services to comply with Regulation (EU) 2016/679 and **the responsibility of supervisory authorities to ensure compliance with that Regulation**." The same specification is **not** made having regard to data altruism organizations.

155. In addition, the EDPB and EDPS consider that, when monitoring compliance, the power of the competent authorities cannot be limited to "the power to request information", as it appears from Article 13(2) of the Proposal. This limitation definitely stems from the declaratory nature of the "labelling regime" envisaged by the Proposal, albeit it is not adequate to the level of vetting the labelling requires, due to the high expectations of data protection compliance resulting from such labelling, especially vis-à-vis data subjects.

156. Finally, the EDPB and EDPS emphasise that adequate resources should be provided to the data protection authorities in order to allow them to effectively and efficiently perform the necessary supervision.

3.5 Data altruism

3.5.1 Interplay between data altruism and consent under the GDPR

157. The concept of "data altruism" referred to in the Proposal covers situations where natural or legal persons make data voluntarily available for reuse, without compensation, for "*purposes of general interest, such as scientific research purposes or improving public services*"[74].

158. It can be argued that the Proposal does not "create" but "formalizes/codifies" the possibility for data holders (defined as including data subjects by the Proposal) to make data available voluntarily, already envisaged in the GDPR. Indeed, a data subject can already consent to the processing of personal data relating to her or him for, among others, scientific research purposes.

159. Despite the definition provided under Article 2(10) of the Proposal ("'data altruism' means the consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services"), the concept of *"data altruism"* is still not clearly and sufficiently defined. In particular, it is unclear whether the consent envisaged in the Proposal corresponds to the notion of "consent" under the GDPR, including the conditions for the lawfulness of such consent. In addition, it is unclear the added value of 'data altruism', taking into account the already existing legal framework for consent under the GDPR, which provides for specific conditions for the validity of consent.

160. The GDPR and the Proposal concurrently apply in case of processing of personal data by data altruism organisations. The EDPB and EDPS support the objective of facilitating the processing of personal data for well-defined purpose(s) of general interest, still such aim shall be achieved in full compliance with the applicable data protection rules and principles. In particular, the EDPB and the EDPS underline that one of the main objectives of the GDPR is to ensure that the data subject keeps control over her or his personal data. In this context, the EDPB and EDPS underline that **all requirements related to the consent, as set in the GDPR, need to be fulfilled**.

161. The EDPB and the EDPS reiterate that **the fundamental right to the protection of personal data cannot in any case be 'waived' by the individual concerned**, be it through an 'act of altruism' related

[74] Article 2(10) of the Proposal.

to personal data. The data controller (the data altruism organisation) remains fully bound by the personal data rules and principles even when the data subject has given consent to the data altruism organisation for the processing of personal data relating to him or her for one or more specified purpose(s).

162. **In light of the above, the Proposal should specify in the substantive part that it refers to consent as defined under Article 4(11) of the GDPR and that, pursuant to Article 7(3), the data altruism organisation shall make as easy to withdraw consent as to provide it[75].**

163. The EDPB and the EDPS also stress the fact that data processed by the data altruism organisations may include special categories of personal data, e.g. data concerning health.

164. The EDPB and the EDPS also underline that, in line with the principle of data minimisation, where it is possible and adequate to the purpose, data should be processed in anonymised form.

165. The EDPB and the EDPS welcome that the Proposal specifies under Article 22(3) that where personal data is provided to the data altruism organisation, the consent form shall ensure that individuals are able to provide and withdraw consent, for a specific data processing operation, in line with the GDPR.

166. In this regard, the EDPB and the EDPS consider that the rules for withdrawal of consent, including its consequences, should be clear. It should be clear in particular how both the data altruism organisation and the data users comply with the requests for withdrawal, including by deleting the personal data in accordance with Article 17(1)(b) GDPR. The EDPB and the EDPS recall that, when taking decisions on 'data altruism', data protection impact assessments may have to be performed by data altruism organizations in accordance with Article 35 of the GDPR.

167. Scientific research often involves the processing and sharing of special categories of personal data on a large scale and thus, in certain cases, the latter could be considered a high-risk data processing according to the GDPR. Furthermore, data protection impact assessments in this context should be conducted with the involvement of the data protection officer (DPO) and of an ethical review board and, where possible and as a matter of good practice, should be made public, or a summary thereof.

168. According to the GDPR, consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

169. Recital 33 of the GDPR underlines that it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects

---

[75] See EDPB Guidelines 5/2020 on consent, at paras 121-122:
"121. Article 6 sets the conditions for a lawful personal data processing and describes six lawful bases on which a controller can rely. The application of one of these six bases must be established prior to the processing activity and in relation to a specific purpose.
122. It is important to note here that **if a controller chooses to rely on consent for any part of the processing, they must be prepared to respect that choice and stop that part of the processing if an individual withdraws consent.** Sending out the message that data will be processed on the basis of consent, while actually some other lawful basis is relied on, would be fundamentally unfair to individuals."

should be allowed to give their consent to certain areas of scientific research when in compliance with recognised ethical standards for scientific research[76]. This is also reflected in recital (38) of the Proposal.

170. However, the EDPB and the EDPS underline that granting this kind of consent for purposes of general interest[77] as such (not strictly defined and referring to a possibly different and much broader scope than scientific research) is not allowed under the GDPR.

171. Indeed, the Proposal, in its recital 35 refers to "purposes of general interest" by providing (not a definition, but) a non-exhaustive list of examples, which includes applied and privately funded research and technological development and data analytics[78].

172. **In light of the above, the EDPB and the EDPS consider that the Commission should better define the purposes of general interest of such "data altruism". The EDPB and EDPS consider that this lack of definition may lead to legal uncertainty, as well as to lower the level of protection of personal data in the EU. For instance, the requirement for the data altruism organization to inform the data holder (including the data subject) "about the purposes of general interest for which it permits the processing of their data by a data user" shall be in line with the principle according to which data shall be collected for specified, explicit and legitimate purposes and not further processed in a**

---

[76] See recently adopted EDPB Guidelines on consent, Guidelines 5/2020, in particular on consent for scientific research, at pages 30-32.

[77] See EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, at paras 42-45:
"42. As a general rule, data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes" pursuant to Article 5 (1) (b) GDPR.
43. However the "compatibility presumption" provided by Article 5(1)(b) GDPR states that "further processing for […] **scientific research purposes** […] shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes". This topic, due to its horizontal and complex nature, will be considered in more detail in the planned **EDPB guidelines on the processing of health data for the purpose of scientific research**.
44. Article 89 (1) GDPR stipulates that the processing of data for research purposes "shall be subject to **appropriate safeguards**" and that those "safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner".
45. The requirements of Article 89(1) GDPR emphasise the importance of the data minimisation principle and the principle of integrity and confidentiality as well as the principle of data protection by design and by default (see below). Consequently, considering the sensitive nature of health data and the risks when re-using health data for the purpose of scientific research, strong measures must be taken in order to ensure an appropriate level of security as required by Article 32(1) GDPR."
See also EDPB document in response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research, adopted on 2 February 2021.

[78] Recital 35: "Such purposes would include healthcare, combating climate change, improving mobility, facilitating the establishment of official statistics or improving the provision of public services. Support to scientific research, including for example technological development and demonstration, fundamental research, applied research and privately funded research, should be considered as well purposes of general interest. This Regulation aims at contributing to the emergence of pools of data made available on the basis of data altruism that have a sufficient size in order to enable data analytics and machine learning, including across borders in the Union."

manner that is incompatible with those purposes (principle of purpose limitation, under Article 5(b) of the GDPR. Hence, an exhaustive list of clearly defined purposes should be provided in the Proposal. At the same time, the EPDB and the EDPS notice the specification made in recital 38 of the Proposal[79]. These specification shall be included in the substantive part of the Proposal and not only in the recital and be accompanied by a clear distinction in the Proposal between:

- consent to areas of scientific research;

- further processing for scientific or historical or statistical purposes;

- and the processing for purposes of general interest (to be defined in the Proposal).

173. Moreover, the EDPB and the EDPS notice that the term "data repositories" in recital (36)[80], referred to only in this recital and not in the substantive part of the Proposal, and related to the processing of both personal and non-personal data, needs to be clarified.

3.5.2 Articles 16-17: registration regime - general requirements to be eligible for registration - content of the registration; outcome (and timing) of the registration;

174. Chapter IV of the Proposal establishes the possibility for organisations engaging in 'data altruism' to register as a "Data Altruism Organisation recognised in the Union"[81] with the declared aim of increasing citizens' trust in their operations. In this regard, the EDPB and EDPS underline that the Proposal does not clarify whether or not the registration is compulsory, nor whether the provisions under Chapter IV also apply in case that organisations engaging in data altruism are not registered.

175. The general requirements for registration are listed in Article 16; the requirements for registration are provided under Article 17, and notably at letters (a)-(i) of Article 17(4). The 'vetting' of the data altruism organization is limited to the verification by the competent authority of the requirements under Article 16 and 17(4) and shall occur within twelve weeks from the date of application. However, the kind of verification with which the competent authority is tasked is not defined by the Proposal.

176. In this respect, the EDPB and the EDPS remark that a regime providing stronger guarantees, in case of processing of personal data, would be more adequate to ensure appropriate checks and ultimately

---

[79] Recital (38): "Data Altruism Organisations recognised in the Union **should be able** to **collect relevant data directly from natural and legal persons or to process data collected by others**.
Typically, data altruism would rely on consent of data subjects in the sense of Article 6(1)(a) and 9(2)(a) and in compliance with requirements for lawful consent in accordance with Article 7 of Regulation (EU) 2016/679.
In accordance with Regulation (EU) 2016/679, **scientific research purposes** can be supported by consent to **certain areas of scientific research** when in keeping with recognised ethical standards for scientific research or only to certain areas of research or parts of research projects.
Article 5(1)(b) of Regulation (EU) 2016/679 specifies that **further processing for scientific or historical research purposes or statistical purposes** should, in accordance with Article 89(1) of Regulation (EU) 2016/679, not be considered to be incompatible with the initial purposes."

[80] Recital (36): "Legal entities that seek to support **purposes of general interest** by making available relevant data based on data altruism at scale and meet certain requirements, should be able to register as 'Data Altruism Organisations recognised in the Union'. This could lead to the establishment of **data repositories**.[...]"

[81] Recital (36) of the Proposal.

enhance trust, than the 'lighter' registration regime (almost a simply 'declaratory' regime) set out in the Proposal and similar to the one envisaged for data sharing service providers.

177. The EDPB and the EDPS underline that the fact that there is almost no requirement from a legal, technical and organizational point of view to become a "Data Altruism Organisation recognised in the Union" (or a "data sharing provider") is problematic. For instance, an organisation, entitled pursuant to Article 15(3) of the Proposal to "refer to itself as a 'Data Altruism Organisation recognised in the Union' in its written and spoken communication" ('labelling effect'), will most probably collect personal data leveraging citizens' expectations in particular on full data protection compliance by the same organisation.

178. The EDPB and the EDPS stress that data altruism organisations need to be trusted entities. As regards the general requirements for registration (provided under Article16 of the Proposal), the EDPB and EDPS also consider that the independence from the for-profit entities of the data altruism organization (e.g. legal, organizational, economical) is envisaged under Article 16(b) the Proposal should to be clarified[82].

179. **In particular, the EDPB and the EDPS recommend introducing a direct reference to data protection requirements in Article 16, especially to the technical and organizational requirements enabling the application of data protection standards and the exercise of data subjects' rights.**

180. **In light of the elements above, and considering the possible impacts for data subjects with regard to the personal data processing that may be undertaken by data altruism organisation, the EDPB and the EDPS consider that the registration regime as laid down in the Proposal does not provide for a sufficiently stringent vetting procedure applicable to such organisation. The EDPB and the EDPS recommend exploring alternative procedures which should notably take into account a more systematic inclusion of accountability and compliance tools for the processing of personal data as per the GDPR, in particular the adherence to a code of conduct or certification mechanism.**

3.5.3 Articles 18-19: transparency requirements and "specific requirements to safeguard rights and interests of data subjects and legal entities as regards their data"

181. The EDPB and the EDPS notice that the requirements accompanying the registration regime should enhance but **not replace the obligations of the data altruism organizations as controllers or processors under the GDPR**.

182. The EDPB and the EDPS notice that recital 36 of the Proposal is unclear in this regard, since it seems to imply that means to withdraw consent shall be provided by the data altruism organization acting as processor[83]. However, the qualification of data altruism organization as processor, instead of

[82] "In order to qualify for registration, the data altruism organisation shall: [...] (b) operate on a not-for-profit basis and **be independent from any entity that operates on a for-profit basis**;" (emphasis added)
[83] Recital 36 laws down (bold added): "**Further safeguards** should include making it possible to **process relevant data within a secure processing environment** operated by the registered entity, **oversight mechanisms** such as ethics councils or boards to ensure that the data controller maintains high standards of scientific ethics, **effective**

controller, needs further assessment, since it does not seem to be the only possible scenario in the context of the Proposal.

183. The enabling effect of the registration (as data altruism organisation) should also be clearly defined, especially having regard to the aspect of the legal basis for the processing of personal data under the GDPR[84]. In this regard, the EDPB and the EDPS reiterate that **the registration regime cannot replace the necessity of an appropriate legal ground for the processing of personal data under Article 6(1) of the GDPR** for the lawfulness of the data processing. In other words, according to the GDPR the processing of personal data shall be lawful only if and to the extent that at least one of the legal basis under Article 6(1) of the GDPR applies

184. Having regard to Article 18 of the Proposal, the EDPB and the EDPS have doubts as to how the independence of the data altruism organisation is preserved in cases where its funding is based on "*the fees paid by natural or legal persons processing the data*"[85] (i.e., data provided to these natural or legal persons by the data altruism organization). In addition, the EDPB and the EDPS consider that the Proposal should better explain in what situations the data altruism organisation can charge fees to natural or legal persons for the processing of the data 'conferred' by data subjects for 'data altruism'.

185. Also in this case, as remarked regarding the re-use of data held by public sector bodies, there is an issue related to incentives for the controller to encourage more processing of personal data, in this case more 'data altruism'. The qualification of data altruism organisations as registered entities having a not-for-profit character (recital 36) -which the EDPB and the EDPS welcome- only partially mitigates the aforesaid issue.

186. Moreover, the wording of recital 36 referring to requirements for data altruism organisations raises concerns since it refers to "voluntary compliance" also with regard to issues related to (mandatory) GDPR compliance[86].

---

technical means to withdraw or modify consent at any moment, **based on the information obligations of data processors under Regulation (EU) 2016/679** as well as **means for data subjects to stay informed** about the use of data they made available." (emphasis added)

[84] In this regard, recital 38 of the Proposal lays down as follows (bold added): "Data Altruism Organisations recognised in the Union **should be able to collect relevant data directly from natural and legal persons** or to process data collected by others. **Typically**, data altruism would rely on consent of data subjects in the sense of Article 6(1)(a) and 9(2)(a) and in compliance with requirements for lawful consent in accordance with Article 7 of Regulation (EU) 2016/679. In accordance with Regulation (EU) 2016/679, scientific research purposes can be supported by consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research or only to certain areas of research or parts of research projects. Article 5(1)(b) of Regulation (EU) 2016/679 specifies that further processing for scientific or historical research purposes or statistical purposes should, in accordance with Article 89(1) of Regulation (EU) 2016/679, not be considered to be incompatible with the initial purposes."

[85] See Article 18(1)(d) of the Proposal.

[86] Recital 36 (bold added): "[...] The **voluntary compliance** of such registered entities with **a set of requirements** should bring trust that the data made available on altruistic purposes is serving a general interest purpose. Such **trust** should result in particular from a **place of establishment within the Union**, as well as from the requirement that registered entities have a **not-for-profit character**, from **transparency** requirements and from **specific safeguards** in place to protect rights and interests **of data subjects and companies**. **Further safeguards** should

187. The recital is also inconsistent (unless prominence is given to the optional nature of the requirements under recital 36) with the substantive part of the Proposal, Article 17(3), which refers to data altruism organisations not established in the Union.

188. **As regards Article 19 of the Proposal, the EDPB and EDPS are of the opinion that an explicit reference to Articles 13 and 14 of the GDPR should be added, in order to ensure consistency between this Article of the Proposal and the obligations concerning the transparency principle under the GDPR, and that the necessary information is provided by the data altruism organisation and by the data users to the data subject with regard to the processing of personal data relating to her or him**.

189. Moreover, the EDPB and the EDPS consider that the current wording of Article 19(1)(a)[87] seems unclear and difficult to reconcile with the provisions of the GDPR .

190. **As regards this Chapter of the Proposal, an explicit emphasis on providing anonymized data when it is possible and adequate for the purpose of data processing, in line with the principle of data minimisation, would also be of special importance to protect persons concerned from undue risks to their fundamental rights and freedoms, especially in case of processing of special categories of data.**

3.5.4 Articles 20 and 21: competent authorities for registration and monitoring of compliance

191. **With regard to article 20(3) of the Proposal, the EDPB and the EDPS consider that the governance and monitoring of compliance should be reinforced in order to ensure a more appropriate vetting of data altruism organizations including compliance with the GDPR, and to ensure that supervision on the provisions of the Proposal is clearly defined in a way that provides that, when it is a matter of personal data, data protection requirements are fully complied with and remain under the competence of the data protection authorities established under the GDPR.**

192. **The designation of data protection authorities as the main competent authorities for the supervision and enforcement of the provisions under Chapter IV of the Proposal would also ensure a more consistent regulatory approach across Member State and therefore contribute to the consistent application of the Proposal. As per their competence and tasks under the GDPR, data protection authorities have already specific expertise in the monitoring of the compliance of data processing, the auditing of specific data processing activities and data sharing, the assessment of the adequate measures to ensure a high level of security for the storage and transmission of personal data, as well as in promoting awareness among controllers and processors of their obligation related to the processing of personal data.**

---

include making it possible to process relevant data within a **secure processing environment** operated by the registered entity, **oversight mechanisms** such as ethics councils or boards to ensure that the data controller maintains high standards of scientific ethics, effective **technical means to withdraw or modify consent** at any moment, based on the information obligations of data processors under Regulation (EU) 2016/679 as well as means for data subjects to **stay informed** about the use of data they made available."

[87] Article 19(1)(a) states (bold added): "Any entity entered in the register of recognised data altruism organisations shall inform data holders: (a) **about the purposes of general interest for which it permits the processing of their data by a data user** in an easy-to-understand manner."

193. In addition, the EDPB and EDPS consider that, when monitoring compliance, the power of the competent authorities cannot be limited to "the power to request information", as it appears from Article 21(2) of the Proposal. This limitation definitely stems from the declaratory nature of the 'labelling regime' envisaged by the Proposal, albeit it is not adequate to the level of vetting the labelling requires, due to the high expectations of data protection compliance resulting from such labelling, especially vis-à-vis data subjects.

194. The EDPB and EDPS emphasise that adequate resources should be provided to the data protection authorities in order to allow them to effectively and efficiently perform the necessary supervision. Furthermore, the EDPB and the EDPS notice in this regard that recital (28) -which refers to providers of data sharing services- states that *"this Regulation should be without prejudice to the obligation of providers of data sharing services to comply with Regulation (EU) 2016/679 and the responsibility of supervisory authorities to ensure compliance with that Regulation."* The same specification should also be made having regard to data altruism organizations.

3.5.5 Article 22: European data altruism consent form

195. Article 22 of the Proposal empowers the Commission to adopt, by means of implementing acts, a "European data altruism consent form" [88]. In this regard, Article 22, as specified under recital 41, provides that the consent form shall be established via an implementing act by the Commission, assisted by the European Data Innovation Board, in consultation with the EDPB.

196. **In this regard, the EDPB and the EDPS consider that a more binding, better structured and institutionalized mechanism than a mere consultation of the EDPB should be established by the Proposal.**

3.6 International transfers of data: Article 5(9)-(13); recital 17, 19; Article 30

197. Even if the provisions of the Proposal relating to data transfers to third countries seem *a priori* limited to only non-personal data, issues of legal and policy consistency with the EU data protection legal framework are likely to emerge during their application, in particular when personal data and non-personal data of a dataset are inextricably linked.

198. However, although the exclusion of personal data seems to be the intention of the Commission, the limitation of the scope of transfers provisions to non-personal data is not always clearly reflected by the Proposal. In particular, Article 5(9) and 5(10), related to transfers of data held by public sector bodies, could apply to personal data if those personal data are at the same time confidential data or data protected by intellectual property rights[89].

---

[88] Article 22(1): "In order to facilitate the collection of data based on data altruism, the Commission may adopt implementing acts developing a European data altruism consent form. The form shall allow the collection of consent across Member States in a uniform format. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 29 (2)."

[89] See Article 5(10) of the Proposal: "Public sector bodies shall only transmit confidential data or data protected by intellectual property rights to a re-user which intends to transfer the data to a third country other than a country designated in accordance with paragraph 9 if the re-user undertakes: (a) to comply with the obligations imposed in accordance with paragraphs 7 to 8 even after the data is transferred to the third country; and (b) to

199. **At the same time, the Proposal includes a provision (Article 5(11)) which could somehow be considered as more "protective" for non-personal data than for personal data, since according to the Proposal the Commission could ultimately adopt, by means of a delegated act[90], specific conditions for the transfer of non-personal data to certain third countries going as far as prohibition[91].**

200. **The possibility for the Commission to adopt, by means of an implementing act[92], 'adequacy decisions' for the transfer of non-personal data to a given third country is also likely to raise questions of interaction and consistency with the transfer tools provided for by the GDPR for the transfer of personal data to the same third country.**

201. **In any case, to ensure consistency with the data protection legal framework, it is important to recall in this regard that in case of 'mixed datasets' the GDPR applies, and in particular its Chapter V.**

202. The EDPB and the EDPS notice that Article 30 of the Proposal[93] refers only to non-personal data and its paragraph 2 seems to mirror the provisions of Article 48 of the GDPR (with the difference that Article 30(2) introduces a limitation in time as to the international agreements concerned).

203. According to Article 30(3) of the Proposal, entities (the public sector body, the entity to which re-use was granted, the data sharing service provider, the data altruism organisation) 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 shall seek the opinion of competent authorities or bodies pursuant to the Proposal in order to determine whether the applicable transfer conditions are met (Article 30(3), last sentence).

204. The consultation of the competent authority is necessary when the decision of the court or of the administrative authority of the third country "would risk putting the addressee in conflict with Union law or with the law of the relevant Member State" (Article 30(3)).[94].

205. This provision, compared with Article 48 GDPR, seems to go one step further by requiring the consultation of the competent authority in specific cases. Therefore, in this regard, it could somehow

---

accept the jurisdiction of the courts of the Member State of the public sector body as regards any dispute related to the compliance with the obligation in point a)."

[90] See recital (19) of the Proposal.

[91] See recital (19) of the Proposal.

[92] See Article 5(9)-(11) of the Proposal.

[93] Article 30, International access, included under Chapter VIII, final provisions.

[94] The aforesaid conditions in Article 30(3) seem sufficient to **supersede the conditions in paragraph (2), and thus supersede the international rules referred to under this paragraph**. Article 30(4) states that: "If the conditions in paragraph 2, **or 3** are met, **the public sector body, the natural or legal person to which the right to re-use data was granted under Chapter 2, the data sharing provider or the entity entered in the register of recognised data altruism organisations, as the case may be, shall, provide the minimum amount of data permissible in response to a request**, based on a reasonable interpretation of the request." (bold added).
These provisions of the Proposal might be i**nconsistent with other Union or member State law, notably on judicial cooperation on criminal or civil matters**. The relevance of this observation under data protection law is given by the fact that **in case of misinterpretation of the notion of non-personal data, there is a high risk of public sector bodies, data sharing service providers, data altruism organizations, data re-users and data users, transferring personal data to a third country with (significantly) lower standard of protection for the persons concerned**.

be considered as more "protective" for non-personal data than for personal data, since such notification is not envisaged under the GDPR.

3.7 Horizontal provisions on institutional settings; complaints; European Data Innovation Board (EDIB) expert group; delegated acts; penalties, evaluation and review, amendments to the single digital gateway regulation, transitional measures and entry into force

3.7.1 Article 23: requirements relating to competent authorities

206. Chapter V of the Proposal sets out the requirements for the functioning of the competent authorities designated to monitor and implement the notification framework for data-sharing service providers and entities engaged in data altruism. It stems from Chapters III and IV of the Proposal that such competent authorities are different from the data protection authorities. Indeed, the requirements established under Article 23 of the Proposal suggest a 'technical' nature of these authorities, *"legally distinct from, and functionally independent of any provider of data sharing services or entity included in the register of recognised data altruism organizations".*

207. In this regard, the role of the data protection supervisory authorities seems limited - under Chapter III - to having a mere exchange of information with the competent authority, and - under Chapter IV- to cooperate with the latter and provide an opinion or decision regarding questions requiring an assessment of compliance with the GDPR, at the request of the competent authority. Moreover, how and to what extent data protection authorities will interact with such competent authorities is not defined by the Proposal, as well as which financial and human resources have been envisaged to allow data protection authorities to carry out the tasks required by such interaction.

208. The EDPB and the EDPS notice that many provisions of the Proposal, whose supervision is assigned to competent authorities, designated pursuant to Article 12 and 20, are related to the protection of personal data. Bearing this in mind, **the EDPB and the EDPS underline that the competences and powers of the independent supervisory authorities shall be fully respected as they are entrusted with the responsibility to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data , as established under the GDPR and EUDPR, in line with Article 16 TFEU and Article 8 of the Charter and in accordance with the relevant case law of the Court of Justice of the European Union[95]. Considering the above, the EDPB and the EDPS recommend that the Proposal explicitly acknowledge that, inasmuch as personal data is involved, data protection authorities are the main competent authorities for the monitoring of the compliance with the provisions under Chapter III and IV of the Proposal, in consultation with other relevant sectorial authorities, when necessary. As already underlined, adequate resources should**

[95] See, among others, Judgment of the ECJ of 9 March 2010, *European Commission v Federal Republic of Germany*, in case C-518/07 available at: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-518/07
In its judgment of 9 March 2010, the Court considered that DPAs should be free from any external influence, whether direct or indirect. The mere risk of an external influence is sufficient to conclude that the DPA cannot act with complete independence.

be provided to these authorities to allow them to effectively and efficiently perform the necessary supervision.

3.7.2 Article 24: complaints; Article 25: right to effective judicial remedy

209. The EDPB and the EDPS notice that Article 24 provides that "*Natural and legal persons shall have the right to lodge a complaint with the relevant national competent authority against a provider of data sharing services or an entity entered in the register of recognised data altruism organisations*", but does not specify the possible content of the complaint (namely, for which violation of the Proposal). It also seems that complaints against public sector bodies or re-users referred to under Chapter II of the Proposal are not possible, not foreseen under Article 24 of the Proposal.

210. In addition, Article 25 lays down 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 the competent authority, as well as with regard to decisions of competent authorities under Articles 13, 17 and 21 (respectively, decision related to supervision on data sharing services; registration of data altruism organisations; monitoring of compliance of registered data altruism organisations).

211. The EDPB and the EDPS observe that the aforesaid provisions of the Proposal on the right to lodge a complaint to the relevant national competent authority (Article 24) and on the right to an effective judicial remedy against failure to act or decisions of aforesaid competent authority (Article 25) might increase the risk, highlighted in this opinion, of parallel and inconsistent regimes between the GDPR and the Proposal. For instance, complaints related to intermediation services which provide data subjects the availability of means to exercise the rights provided under the GDPR (see Article 9(1)(b)) would fall under the remit of the competent authorities under the Proposal. In other words, the 'substantive law' inconsistencies and overlaps would also 'escalate' into administrative and judicial proceedings' overlaps of competences.

212. For this reason, **the EDPB and the EDPS call for a clear, unambiguous and rigorous definition of the substantive rules of the Proposal whose supervision is assigned to competent authorities, and of its monitoring mechanism, which ensures full consistency with the GDPR**.

3.7.3 Articles 26 and 27: composition and tasks of the European Data Innovation Board Expert Group

213. Chapter VI of the Proposal *"creates a formal expert group (the 'European Data Innovation Board') with the task of facilitating the emergence of best practices by Member States' authorities in particular on processing requests for the re-use of data which is subject to the rights of others (under Chapter II), on ensuring a consistent practice regarding the notification framework for data sharing service providers (under Chapter III), and for data altruism (Chapter IV). In addition, the formal expert group will support and advise the Commission on the governance of cross-sectoral standardisation and the preparation of strategic cross-sector standardisation requests"*[96].

[96] Explanatory Memorandum, page 8.

214. The EDPB and the EDPS notice that the newly established European Data Innovation Board, "*consisting of the representatives of competent authorities of all the Member States, the European Data Protection Board, the Commission, relevant data spaces and other representatives of competent authorities in specific sectors*" (Article 26(1)) would be entrusted with the tasks listed under Article 27, letters (a)-(e)[97], which are also relevant having regard to the processing of personal data.

215. **The EDPB and the EDPS welcome the inclusion of the EDPB as a member of the European Data Innovation Board. However, the EDPB and the EDPS consider that the provisions related to the European Data Innovation Board are likely to impinge, insofar as relating to the processing of personal data, on the tasks and competences of national data protection authorities and of the EDPB to protect the fundamental rights and freedoms of natural persons and to facilitate the free flow of personal data within the Union[98] (having regard in particular to the wide range of tasks entrusted to the EDPB under Article 70 of the GDPR to advise the Commission and to issue guidelines, recommendations and best practices, and to the tasks entrusted to the EDPS under Article 57 of the EUDPR).**

216. **Therefore, the EDPB and the EDPS recommend clarifying in the legal text that the data protection supervisory authorities established under national and Union law are the "competent authority", insofar as the processing of personal data is concerned. In addition, it should be clear that the provision of advice to the European Commission regarding data protection matters and the development of consistent practices related to the processing of personal data do not fall within the competences attributed to the European Data Innovation Board, since article 70 GDPR explicitly confers those tasks to the EDPB.**

217. **The EDPB and the EDPS also recommend, for precision and legal clarity, as well as avoidance of possible misunderstanding, renaming the European Data Innovation Board as "Commission Expert**

---

[97] "The Board shall have the following tasks:
(a) to advise and assist the Commission in developing a consistent practice of public sector bodies and competent bodies referred to in Article 7(1) **processing requests for the re-use of the categories of data referred to in Article 3(1)**;
(b) to advise and assist the Commission in developing a consistent practice of the competent authorities in the application of **requirements applicable to data sharing providers**;
(c) to advise the Commission on the **prioritisation of cross-sector standards to be used and developed for data use and cross-sector data sharing**, cross-sectoral comparison and exchange of best practices with regards to sectoral requirements for security, access procedures, while taking into account sector-specific standardisations activities;
(d) to assist the Commission in **enhancing the interoperability of data as well as data sharing services** between different sectors and domains, building on existing European, international or national standards;
(e) to facilitate the cooperation between national competent authorities under this Regulation through capacity-building and the exchange of information, in particular by establishing methods for the efficient exchange of information relating to the notification procedure for data sharing service providers and the registration and monitoring of recognised data altruism organisations."

[98] See for instance Article 27(a), according to which the Board shall have the task to "advise and assist the Commission in developing a consistent practice of public sector bodies and competent bodies referred to in Article 7 (1) processing requests for the re-use of the categories of data referred to in Article 3 (1);" (emphasis added)

Group on Data Governance" or similar, to better reflect the *legal status* and the *nature* of the body established under Article 26 of the Proposal.

3.7.4 Article 31: penalties for infringements of the Proposal, to be applied

218. **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**), providing that *"Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall notify the Commission of those rules and measures by [date of application of the Regulation] and shall notify the Commission without delay of any subsequent amendment affecting them*."

219. 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 increase trust in re-use, data sharing services and data altruism.

3.7.5 Article 33: amendment to Regulation (EU) 2018/1724

220. This Article of the Proposal amends the single digital gateway regulation (Regulation (EU) 2018/1724)[99], introducing the following administrative procedures: notification as provider of data sharing services; registration as a European Data Altruism Organization. The expected outcome of which is, respectively: confirmation of the receipt of the notification, confirmation of the registration.

221. **In this regard, the EDPB and the EDPS observe that the notification and registration regime, already analysed in this Opinion, cannot replace the necessity of an appropriate legal ground for the processing of personal data under Article 6(1) of the GDPR for the lawfulness of the data processing. In other words, according to the GDPR the processing of personal data shall be lawful only if and to the extent that an adequate legal basis under Article 6(1) of the GDPR applies. The Proposal should clearly specify this aspect to avoid any ambiguity.**

Brussels, 10 March 2021

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

[99] Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (Text with EEA relevance.), OJ L 295, 21.11.2018, p. 1–38.