EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space

Adopted on 12 July 2022

TABLE OF CONTENTS

Executive Summary

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

The EDPB and the EDPS note that the Proposal aims at supporting individuals to take control of their own health data, supporting the use of health data for better healthcare delivery, better research, innovation and policy making, and enabling the EU to make full use of the potential offered by a safe and secure exchange, use and reuse of health data. Indeed, 'facilitating the use of electronic health data', both for primary and secondary use of electronic health data could significantly contribute to both public interests, as well as to the interest of individual data subjects/patients.

Although the effort to strengthen the control and rights of data subjects over their personal health data is welcomed, it should be highlighted that this Proposal mainly provides for some 'add-ons' to some of the rights of data subjects already provided for in the GDPR. In fact, the Proposal may even weaken the protection of the rights to privacy and to data protection, especially considering the categories of personal data and purposes that are related to the secondary use of data.

The EDPB and the EDPS note that the provisions in this Proposal will add yet another layer to the already complex (multi-layered) collection of provisions (to be found both in the EU and Member States law) on the processing of health data (in the health care sector). The interplay between those different pieces of legislation needs to be (crystal) clear.

In particular, the EDPB and the EDPS consider that it is important to clarify the relationship between the provisions in this Proposal with the ones in the GDPR and Member State laws. The EDPB and the EDPS acknowledge the intention and efforts to stay within the boundaries of the GDPR in this EHDS Proposal. This can be recognised, for instance, when it creates, by means of Union law, legal grounds and/or exceptions for the processing of health data fitting into the structure of the GDPR foreseen in Articles 6 and 9 GDPR. However, as to the desired level of clarity of those provisions, much is still called for (by way of improvement of provisions and further clarification), especially in regard to the interplay of the provisions with Member State laws pursuant to Article 9(4) GDPR. Those concerns are reflected in the comments on both the Chapters II and IV of the Proposal.

With regards to the scope of the Proposal, the EDPB and the EDPS recommend excluding from Article 33(1)(f) of the Proposal respectively wellness applications and other digital applications, as well as wellness and behaviour data relevant to health. Should these data be maintained, the processing for secondary use of personal data deriving from wellness applications and other digital applications should be subject to prior consent within the meaning of the GDPR. Moreover, the EDPB and the EDPS recall that such processing may fall within the scope of Directive 2002/58/EC ('e-Privacy Directive').

The EDPB and the EDPS also strongly recommend to not extend the scope of the GDPR exceptions regarding the data subject's rights to the Proposal and in particular in Article 38(2) of the Proposal. Such exemption undermines the possibility for data subjects to exercise an effective control over their personal data rather than strengthen it and thus appears to be at odds with the objective laid down in Article 1(2)(a) of the Proposal.

The EDPB and the EDPS welcome that fact that the Proposal makes reference to GDPR rights (e.g. the right of access free of charge, and the right to obtain a copy of the data). However, the EDPB and the EDPS note that the description of the rights as provided in the Proposal is not consistent with the one of the GDPR. As mentioned above, this may lead to legal uncertainty vis-a-vis the data subjects who may not be able to

distinguish between the two types of rights. To this purpose, and in order to avoid complexities of practical implementation, the EDPB and the EDPS urge the co-legislator to ensure legal clarity on the interplay between the data subject's rights introduced by the Proposal and the general provisions contained in the GDPR on data subject's rights.

The EDPB and the EDPS acknowledge the provisions in Chapter III that aim to improve the interoperability of Electronic Health Records and to facilitate the connectivity of wellness-apps with such electronic health records. However, the EDPB and the EDPS are of the opinion that the latter should not be included in the secondary use of health data under Chapter IV of the Proposal. First, because health data generated by wellness applications and other digital health applications do not have the same data quality requirements and characteristics of those generated by medical devices. Moreover, these applications generate an enormous amount of data and can be highly invasive since it relates to every step individuals takes in their everyday lives. Even if health data could be indeed separated from other kinds of data, inferences such as food practices and other habits could be easily made, revealing particularly sensitive information such as religious orientation.

As to the purposes for secondary use of health data listed under Article 34(1) of the Proposal, the EDPB and the EDPS understand that Articles 34(1)(f) and (g) of the Proposal possibly encompass any form of 'development and innovation activities for products or services contributing to public health or social security' or 'training, testing and evaluation of algorithms, including in medical devices, AI systems and digital health applications, contributing to public health or social security'. The EDPB and the EDPS are of the view that the Proposal should further delineate these purposes and circumscribe when there is a sufficient connection with public health and/or social security. This will be crucial to achieve a balance adequately taking into account the objectives pursued by the Proposal and the protection of personal data of the data subjects affected by the processing.

In addition, Article 34(1) of the Proposal contain several types of secondary use, which would fall under different categories of grounds for exception foreseen in Article 9(2) GDPR. However, the EDPB and the EDPS consider that this is not reflected in the criteria according to which the health data access bodies should assess and decide on data applications (Article 45 of the Proposal) in order to issue a data access permit (Article 46 of the Proposal). To this end, the EDPB and the EDPS highlight that the criteria provided for in this regard by Article 46 of the Proposal are restricted to the provisions and principles of this Proposal and lack clarity as to the way such provisions relate to the principles and provisions of the GDPR, in particular to Article 9(2) GDPR.

In relation to Chapter V, the EDPB and the EDPS acknowledge that the infrastructure for the exchange of electronic health data foreseen in this EHDS-proposal in no way is aimed at (or could result in) establishing a central EU-database of health data and will only facilitate the exchange of such health data from decentralised databases. However, due to the large quantity of data that would be processed, their highly sensitive nature, the risk of unlawful access and the necessity to fully ensure effective supervision over these data, the EDPB and the EDPS call for adding to this Proposal a provision that would require storing the personal electronic health data in the EU/EEA, without prejudice to further transfers in compliance with Chapter V of the GDPR.

Finally, regarding the governance model created by the Proposal, the tasks and competences of the new public bodies need to be carefully tailored, particularly taking into account the tasks and competences of national Supervision Authorities, the EDPB and the EDPS in the field of processing personal (health) data. Overlap of competences should be avoided and fields of and requirements for cooperation should be specified.

The European Data Protection Board and the European Data Protection Supervisor

Having regard to Article 42(2) of the Regulation 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC,

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

HAVE ADOPTED THE FOLLOWING JOINT OPINION

1 BACKGROUND

1. The Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space Act ("the Proposal") will help to attain the Commission's vision for EU's digital transformation by 2030[1].

2. The European Data Protection Board ("EDPB") and the European Data Protection Supervisor ("EDPS") note that, according to the Commission, the Proposal "*supports individuals to take control of their own health data, supports the use of health data for better healthcare delivery, better research, innovation and policy making and enables the EU to make full use of the potential offered by a safe and secure exchange, use and reuse of health data*"[2].

3. As explained in the Explanatory Memorandum, the Proposal is in line with the EU's overarching objectives. Such objectives include the creation of a stronger European Health Union, implementing the European Pillar of Social Rights, improving the functioning of the internal market, promoting synergies with the EU digital internal market agenda and delivering an ambitious research and innovation agenda. Furthermore, the Proposal will provide an important set of elements contributing to the formation of the European Health Union, by encouraging innovation and research and dealing better with future health crises.

2 SCOPE OF THE OPINION

4. On 3 May 2022, the Commission published the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space Act ("the Proposal").

[1] Explanatory Memorandum, p. 2.
[2] https://ec.europa.eu/health/ehealth-digital-health-and-care/european-health-data-space_en

5. On 4 May 2022, the Commission requested a Joint Opinion of the EDPB and the EDPS ("the Opinion") on the basis of Article 42(2) of Regulation (EU) 2018/1725[3] ("EUDPR") on the Proposal.

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

7. The EDPB and the EDPS welcome the explanatory memorandum of the Proposal, where it is stated that "*considering that a substantial amount of electronic data to be assessed in the EHDS are personal health data relating to natural persons in the EU, the proposal is designed in full compliance not only with the GDPR but also with Regulation (EU) 2018/1725 (EU Data Protection Regulation)".*

8. Along the same lines, the EDPB and the EDPS highlight that it is necessary to ensure and uphold the respect and the application of the EU acquis in the field of data protection. When personal data are involved in the context of the Proposal, it is essential to clearly avoid in the legal text of the Proposal any inconsistency and possible conflict with the General Data Protection Regulation[4] ("GDPR"), the ePrivacy Directive[5] and the EUDPR. This not only for the sake of legal certainty, but also to avoid that the Proposal has the effect of directly or indirectly jeopardising the fundamental rights to privacy and protection of personal data, as established under Articles 7 and 8 of the Charter of fundamental rights of the European Union (the "Charter") and Article 16 of the Treaty on the Functioning of the European Union ("TFEU").

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

3 ASSESSMENT

3.1 General remarks

10. The EDPB and the EDPS acknowledge the objective of the Proposal to expand the use of electronic health data to deliver health care to the individual from whom those data were collected ("primary use") and to improve research, innovation, policy making, patient safety, personalised medicine, official statistics or regulatory activities ("secondary use"). The EDPB and the EDPS also acknowledge

[3] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ, 21.11.2018, L.295, p. 39.
[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p. 1–88.
[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p. 37–47.

the Proposal's goal to improve the functioning of the internal market by laying down a uniform legal framework for the development, marketing and use of electronic health record systems ("EHR systems").

11. Nevertheless, the EDPB and the EDPS highlight that the protection of personal data is an integral element of the trust individuals and organisations should have in the development of the digital economy[6] and the access to equitable health care, in particular in the context of processing health data within the EHDS framework.

12. In this regard, the EDPB and the EDPS underline that the success of the EHDS will depend on a robust legal basis for processing in line with EU data protection law, the establishment of a strong data governance mechanism and effective safeguards for the rights and interests of natural persons that are fully compliant with the GDPR. Sufficient assurances of a lawful, responsible, ethical management anchored in EU values, including respect for fundamental rights, should be provided. In this regard, the EDPB and the EDPS consider that the EHDS should serve as an example of transparency, effective accountability and proper balance between the interests of the individual data subjects and the shared interest of society as a whole.

13. In the forthcoming chapters of the Opinion, the EDPB and the EDPS provide recommendations on how to make the relevant provisions of the Proposal not only compliant with the EU data protection legal framework, but also in line with the current interpretation of the applicable jurisprudence of the Court of Justice of the European Union ("CJEU"). Given the wide scope of the rights and obligations set out in the Proposal with regard to the access, use and sharing of special categories of personal data as is the case for health data, general references to the GDPR and the EUDPR may not suffice. In this regard, the EDPB and the EDPS consider that there may be a risk of misinterpreting key provisions related to data protection which, in turn, may lead to a lowering of the level of protection currently granted to data subjects under the existing EU data protection legal framework (GDPR, EUDPR and ePrivacy Directive). Therefore, the EDPB and the EDPS consider further specifications necessary, as will be detailed in the remainder of this Opinion.

14. The EDPB and the EDPS positively note that the Proposal also aims at contributing to a mitigation of the current fragmentation of rules applicable to the processing of health data and to scientific research. At the same time, the EDPB and the EDPS raise doubts about the full compatibility of some of the provisions of Chapter II and IV of the Proposal (notably the access by health professionals to restricted personal electronic health data, the systematic registration of the relevant health data by health professionals or the handle of unexpected findings by health data access bodies towards natural persons) with Member State law in the e-health sector, in the absence of a general EU legislative competence of harmonisation in this domain. In this regard, it should be recalled that under Article 168 TFEU, Union action shall encourage cooperation between the Member States in the area of public health and, if necessary, lend support to their action by complementing national policy while respecting the responsibilities of the Member States for the definition of their health policy and for the organisation and delivery of health services and medical care.

3.2 Interplay of the Proposal with EU data protection law

15. The EDPB and the EDPS welcome Recital 4 of the Proposal, according to which "*[p]rocessing of personal electronic health data is subject to the provisions of Regulation (EU) 2016/679 of the*

[6] DGA Joint Opinion.

European Parliament and of the Council and, for Union institutions and bodies, Regulation (EU) 2018/1725 of the European Parliament and of the Council. References to the provisions of Regulation (EU) 2016/679 should be understood also as references to the corresponding provisions of Regulation (EU) 2018/1725 for Union institutions and bodies, where relevant".

16. Moreover, according to the Explanatory Memorandum, the Proposal is based on Articles 114 and 16 of the Treaty on the Functioning of the European Union ('TFEU'). In the light of the Proposal, while Article 114 TFEU aims at improving the functioning of the internal market through measures for the approximation of national rules, the Proposal aims at expanding the use of electronic health data while strengthening the rights arising from Article 16 TFEU.

17. In this regard, the EDPB and the EDPS, in line with the CJEU's jurisprudence, highlight that Article 16 TFEU provides for an appropriate legal basis in cases where the protection of personal data is one of the essential aims or components of the rules adopted by the EU legislator[7]. Moreover, the EDPB and the EDPS recall that the application of Article 16 TFEU also entails the need to ensure independent oversight for compliance with the requirements regarding the processing of personal data, as is also required by Article 8 of the Charter[8].

18. Indeed, with reference to the point made on independent oversight, the EDPB and the EDPS highlight that, according to Recital 43 of the Proposal, supervisory authorities should be tasked with enforcing the relevant provisions of the GDPR and EUDPR especially with regard to the processing of personal data for secondary uses in the context Chapter IV of the Proposal. In this regard, the EDPB and the EDPS recommend including a corresponding provision in the operative part of the text.

19. Concerning the recourse to Article 16 TFEU as (one of the two[9]) legal basis of the Proposal, the EDPB and the EDPS acknowledge that the **aim** of the Proposal is to specify 'additional legally binding provisions and safeguards[10]' in relation to the protection of health data. Such provisions are 'additional' to those of the GDPR. The Proposal provides for 'specific requirements and standards'[11] which are tailor-made for electronic health data processing and are intended to 'bring to reality the possibility offered by the GDPR for an EU law for several purposes'[12].

20. As to the **content** of the Proposal**,** the EDPB and the EDPS wish to put forward two general remarks.

21. Firstly, the Proposal contains predominantly rules on the processing of personal (health) data, be it for primary or secondary use. Having regard to the impact of these provisions on the overall center of gravity of the Proposal, the EDPB and the EDPS agree that the content of the Proposal makes of Article 16 TFEU a necessary legal base. This is without prejudice to the comments in the present Opinion on the interaction of several provisions of the Proposal with those of the GDPR, an interaction which strongly calls for further clarifications and, sometimes, further reflection and reworking, as developed later in this Opinion.

---

[7] Opinion of 26 July 2017, PNR Canada, Opinion procedure 1/15, ECLI:EU:C:2017:592, paragraph 96.
[8] AI Act JO.
[9] The EDPS and the EDPB, in line with their mandates, will not deal in this Opinion with the matter of the justification of recourse to a double legal base and will limit themselves to considerations relating to recourse to Article 16 TFEU.
[10] Explanatory Memorandum to the Proposal, p. 6.
[11] Ibidem.
[12] Ibidem.

22. The EDPB and the EDPS also note that, according to Recital 37, this Proposal aims to provide Union law making use of the exceptions in Articles 9(2)(g), (i) and (j) GDPR. The EDPB and the EDPS also note that, for the secondary use of health data, the Proposal creates an obligation for data holders in the sense of Article 6(1)(c) GDPR to disclose personal data to health data access bodies. At the same time, the EDPB and the EDPS understand that the Proposal does not aim to create a legal basis for data applicants in relation to Article 6 GDPR nor modify information requirements under the GDPR or the ePrivacy Directive, or alter any rights set out therein.

23. Secondly, the EDPB and the EDPS note that the Proposal contains at least one explicit derogation from a provision of the GDPR: Article 38(2) of the Proposal indeed exempts certain entities (the health data access bodies) from applying the provisions of Article 14 GDPR concerning information to be provided to data subjects. The EDPB and EDPS consider that such exemption undermines the possibility for data subjects to exercise an effective control over their personal data rather than strengthen it and thus appears to be at odds with the objective laid down in Article 1(2)(a) of the Proposal. Moreover the EDPB and the EDPS question whether it is necessary and justified to introduce a restriction to the right of information as further explained in Paragraphs 26, 34, 96 and 97 of this Opinion, also in the light of Article 23 GDPR.

24. More generally, the EDPB and the EDPS caution against legislation laying down derogations from the tasks and powers of data protection supervisory authorities and the generally applicable rules of the GDPR in accordance with article 8 of the Charter. Such legislation inevitably affect, and ultimately has the potential to undermine, over time, the centrality of the horizontal rules adopted under Article 16 TFEU. The independent supervisory authorities should be tasked with the oversight of the Proposal, insofar as the processing of personal data is concerned.

25. In any event, the EDPB and EDPS question whether a restriction to the right of information is necessary and justified in this context. Indeed, both Article 14(5)(b) and Article 14(5)(c) GDPR exempts controllers from complying with Article 14 GDPR in certain cases, namely where (1) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or insofar as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing[13]; and (2) where the obtaining or disclosure of personal data is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interest. Insofar as the EHDS Proposal expressly provides for obtaining or disclosure of personal data, it should rather be assessed whether this Proposal contains appropriate safeguards to protect data subjects' legitimate interests.

26. Finally, the EDPB and the EDPS note that, although the Proposal also covers wellness applications and other digital health applications, the ePrivacy Directive is not included in its Article 1(4). While the EDPB and the EDPS question the inclusion of such applications within the scope of Chapter IV of the Proposal, as will be explained in the next Chapter, the EDPB and the EDPS recommend including a reference to the ePrivacy Directive, should these applications still be part of the Proposal.

[13] In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

27. Moreover, Article 1(4) of the Proposal should also make reference to the EUDPR and the relevant provisions of the EUDPR should also be identified explicitly throughout the Proposal[14]. Explicit references to the relevant EUDPR articles in the enacting terms of the Proposal appear more than warranted, first because the Commission will act as processor for electronic health data communicated through 'MyHealth@EU' (Article 12(7) of the Proposal), secondly, because Union institutions, bodies, offices and agencies may have regular access to electronic health data (Recital 41 of the Proposal) and, thirdly, since data held by EUIs may also be made available for secondary use (Recital 46 of the Proposal).

3.3 Interplay of the Proposal with the DGA, the Data Act and the AI Act

28. The EDPB and the EDPS note that, in line with Article 1(4) of the Proposal, "[*t]he Regulation shall be without prejudice to other Union legal acts regarding access to, sharing of or secondary use of electronic health data, or requirements related to the processing of data in relation to electronic health data, in particular Regulations (EU) 2016/679, (EU) 2018/1725, […] [Data Governance Act COM/2020/767 final] and […] [Data Act COM/2022/68 final*]." Moreover, in line with Article 1(5) of the Proposal, the "(...) *Regulation shall be without prejudice to Regulations (EU) 2017/745 and […] [AI Act COM/2021/206 final], as regards the security of medical devices and AI systems that interact with EHR systems*".

29. While welcoming the explicit reference to the Proposal being without prejudice to the Data Governance Act ("DGA"), the Data Act and the Artificial Intelligence ("AI") Act, the EDPB and the EDPS consider that the specific interaction of the Proposal with the aforementioned initiatives part of the digital package as well as the Medical Devices Regulation (MDR)[15], should be better addressed. To illustrate this point and only as an example, the Proposal introduces a definition of 'data holder' under Article 2(2)(y) which might not be consistent with the definition of data holder in the DGA and the Data Act. This might lead to legal uncertainty as to what entities would fall within such definition, despite constituting a central aspect of the Proposal, given that it would - crucially - determine which entities will be subject to the obligation of making electronic health data available for secondary use.

30. The EDPB and the EDPS further note that the general objective of the Proposal is to ensure that natural persons in the EU have increased control over their electronic health data which cannot be achieved if the interplay between the relevant regulations is not clearly identified. Legal certainty is key not only to ensure that the different stakeholders feel safe to act within the new framework, but also that the rights of natural persons are guaranteed. Therefore, the EDPB and the EDPS recommend further clarifying the interplay of the Proposal with the above-mentioned initiatives and legal instruments.

4 GENERAL PROVISIONS (CHAPTER I)

[14] In accordance with Recital (4) of the Proposal, references to the provisions of GDPR should be understood also as references to the corresponding provisions of the EUDPR. While the aim of Recital (4) is clear, the EDPB and EDPS strongly recommend that the relevant provisions of the EUDPR be identified explicitly in the enacting terms of the Proposal as such.

[15] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, 5.5.2017, L 117/1.

4.1 Article 1: Subject matter and scope of the Proposal

31. The EDPB and the EDPS welcome that the Proposal aims, amongst others, at strengthening the rights of natural persons in relation to the availability and control of their electronic health data.

32. The EDPB and the EDPS are aware that the COVID-19 pandemic has greatly accelerated the use of medical devices, wellness applications or wearables amongst the general population. However, this kind of technology generates an enormous amount of data, often special categories of personal data, and can be highly invasive. More than tracking humans' actions and decisions, it is now possible to track humans' bodies, minds and emotions at a level that even humans themselves might not be able to do. These data can then be used to predict people's actions and manipulate their behaviour, even at a group level.

33. The EDPB and the EDPS note that, as laid down in Article 1(2)(a) of the Proposal, the first objective of the Proposal is to strengthen the rights of natural persons in relation to the availability and control of their electronic health data. At the same time, the EDPB and the EDPS also note that, unlike in the primary use, for which the Proposal allows natural persons to restrict the access to their personal data, the same option is not afforded with regard to secondary use of data. Moreover, under Article 38(2) of the Proposal, "[*h]ealth data access bodies shall not be obliged to provide the specific information under Article 14 of Regulation (EU) 2016/679 to each natural person concerning the use of their data for projects subject to a data permit* (...)". The EDPB and the EDPS underline that the right to information and the right to object are inextricably linked. By restricting the right to information under the GDPR, the EDPB and the EDPS are of the view that the Proposal may not achieve the objectives laid down in Article 1(2)(a) of the Proposal. In fact, the envisaged approach appears to undermine the rights of natural persons to privacy and to the protection of personal data, especially taking into account the very broad definition of secondary use and the minimum categories of electronic data for secondary use introduced by the Proposal, which is not only limited to scientific research but also includes other purposes, such as innovation.

34. In addition, the EDPB and the EDPS note that Article 1(3)(a) of the Proposal provides that the Proposal applies to "(...) *manufacturers and suppliers of* ***EHR systems*** *and* ***wellness applications*** *placed on the market and put into service in the Union and the users of such products* ", while Article 33(1)(f) and (n) of the Proposal lists among the minimum categories of electronic data for secondary use person generated electronic health data, including **medical devices, wellness applications or other digital health applications, as well as wellness and behaviour data relevant to health** (emphasis added). First, there is an inconsistency between the scope of the Proposal and the categories of data listed under Article 33 (1)(f) of the Proposal: the former refers to manufacturers and suppliers of EHR systems and wellness applications only, while the latter also includes medical devices on top of wellness applications and other digital health applications. The EDPB and the EDPS are of the understanding that medical devices also fall within the scope of the Proposal. Thus, for the sake of legal clarity, the EDPB and the EDPS recommend adding manufacturers and suppliers of medical devices in Article 1(3)(a) of the Proposal.

35. Furthermore, the EDPB and the EDPS highlight that health data generated by wellness applications and other digital health applications do not have the same data quality requirements and characteristics of those generated by medical devices (the latter being subject to existing specific standards and legislation). Moreover, it should be noted that digital health applications may possibly gather personal data that go beyond health data: for instance, the collection of personal information

regarding food practices and other habits may indirectly reveal particularly sensitive information such as religious orientation.

36. Against this background, while the EDPB and the EDPS understand the possible need of including medical devices within the scope of the Proposal, **the EDPB and the EDPS recommend excluding from Article 33(1)(f) and (n) of the Proposal respectively wellness applications and other digital applications, as well as wellness and behaviour data relevant to health**. Should these data be maintained, the processing for secondary use of personal data deriving from wellness applications and other digital applications should be subject to prior consent within the meaning of the GDPR. Moreover, the EDPB and the EDPS recall that such processing may fall within the scope of Directive 2002/58/EC ('e-Privacy Directive').

37. The EDPB and the EDPS note that, according to Article 2(2) of the Proposal, the definition of data holder explicitly includes European Union Institutions ('EUIs'). However, **EUIs can be both a controller of personal and health related data (and thus a data holder) as well as a data user of personal and health related data**[16]. This is explained in Recital 41 and Articles 34, 45 and 48 of the Proposal. As a result, and for the sake of legal certainty, the EDPB and the EDPS **recommend clarifying whether the EUIs are included in the definition of data user as well**. Lastly, the EDPB and the EDPS recall that, as Union institutions, bodies, offices and agencies are not subject to national jurisdictions, specific clarification should be made in relation to the penalties that can be imposed by health data access bodies, as provided for in Article 43 of the Proposal.

4.2 Article 2: Definitions

38. The EDPB and the EDPS note that Article 2 of the Proposal provides relevant definitions for the understanding of the Regulation as a whole. However, the EDPB and the EDPS consider that several of them are very broad and open to interpretation, which in turn may lead to legal uncertainty.

39. Firstly, Article 2(1)(1) of the Proposal states that the **definitions in Regulation (EU) 2016/679** shall apply. At the same time, the Proposal introduces new definitions and refers to specific concepts in other regulations, such as the Data Act. For instance, the Proposal introduces a defintion of 'data recipient' although such definitiondefinition is already provided in Article 4(9) of the GDPR. Since the Proposal aims to complement certain GDPR provisions, for the sake of legal certainty, the EDPB and the EDPS recommend explaining why additional definitions are necessary, or in the most extreme case, by way of exception, identify those GDPR definitions that do not apply.

[16] EU institutions, bodies and agencies process health related data mainly in the following contexts:
1. recruitment (pre-recruitment medical examination),
2. occupational health (annual medical visit) / health and safety at work,
3. reimbursement of medical expenses (Joint Insurance Sickness Scheme),
4. sick leaves (medical certificates) and invalidity procedures, and
5. performance of a task vested in the EUI's mission (e.g. European Centre for Disease Prevention and Control and European Medicines Agency).

Processing operations involving health data are likely to present specific and higher risks to the rights and freedoms of data subjects, who are staff members, temporary agents, contractual agents, national experts, trainees of these bodies, candidates for the positions mentioned before and visitors of the EUIs. Those risks are similar to the ones data subjects face when their health data is processed by controllers that are not EUIs.

40. Article 2(2)(a) of the Proposal defines **'personal electronic health data'** as data concerning health and genetic data as defined in the GDPR, as well as data referring to determinants of health, or data processed in relation to the provision of healthcare services, processed in an electronic form. In this regard, it is worth underlining that Recital 35 GDPR already includes 'information collected in the course of the provision of health care services'. In addition Recital 54 of the Proposal also refers to 'determinants having an effect on that health status', in particular in the context of the processing of such data concerning health for reasons of public interest. To ensure as much alignment with the GDPR as possible, the EDPB and EDPS recommend to amend the definition in Article 2(2)(a) of the Proposal to simply refer to "data concerning health and genetic data as defined in Regulation (EU) 2016/679 that are processed in an electronic form".

41. On the other hand, Article 2(2)(b) of the Proposal defines '**non-personal electronic health data'** as data concerning health and genetic data in electronic format that falls outside the definition of personal data provided in Article 4(1) GDPR. In this regard, the EDPB and the EDPS once again[17] underline that the distinction between categories of personal and non-personal data is difficult to apply in practice. Indeed, 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, especially when non-personal data are the result of the anonymisation of personal data and even more in the context of processing of health data. Against this background, the EDPB and the EDPS take note of the risk of re-identification set out in Recital 64 of the Proposal and recommend to make more explicit that in case of mixed datasets (whereby personal and non-personal data are "inextricably linked") the protections of the GDPR and the Proposal concerning personal electronic health data shall be applicable.

42. Articles 2(2)(d) and 2(2)(e) of the Proposal define the '**primary use of electronic health data'** and the **'secondary use of electronic health data'** respectively. The EDPB and the EDPS consider that these definitions may give rise to legal uncertainty and inconsistency with the GDPR, in particular with regard to the definition of secondary use of electronic health data. In particular, the second part of Article 2(2)(e) of the Proposal states that "*[t]he data used may include personal electronic data initially collected in the context of primary use, but also electronic data collected for the purpose of secondary use."* The EDPB and the EDPS consider that, as the concept of 'secondary use of personal data' does not appear in the GDPR, the second part of the definition of 'secondary use of electronic health data' deviates from the GDPR concept of 'further processing of personal data'. In fact, the latter is to be understood in relation to the purpose for which a particular controller originally collected the data, irrespective of their qualitative aspects. As a result, the EDPB and the EDPS recommend to correct such definitions in the light of the GDPR, and in particular to clarify the link between the definition of secondary use of electronic health data within the meaning of the Proposal and the concept of 'further use of personal data' within the meaning of the GDPR, especially taking into account the special regime already afforded by the GDPR to scientific research.

43. Article 2(2)(f) of the Proposal defines **'interoperability**' as the "*ability of organisations as well as software applications or devices from the same manufacturer or different manufacturers to interact towards mutually beneficial goals, involving the exchange of information and knowledge without changing the content of the data between these organisations, software applications or devices, through the processes they support*". In this regard, the EDPB and the EDPS consider that such

[17] EDPB-EDPS Joint Opinion on the DGA Act, para.58.

definition may need additional clarification as to its interplay with alreadyalready-existing definitions of interoperability in other legislation such as the DGA and the eIDAS Regulation.

44. Article 2(2)(y) of the Proposal defines a **'data holder'** as "*any natural or legal person, which is an entity or a body in the health or care sector, or performing research in relation to these sectors, as well as Union institutions, bodies, offices and agencies who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data, through control of the technical design of a product and related services, the ability to make available, including to register, provide, restrict access or exchange certain data.*" As already underlined above in paragraph 29, this is a central definition, which however is so broad that does not allow to clearly identify who would qualify as data holder[1] and to understand what the interplay is with the definition of data holder provided in the Data Act and the DGA. If this provision does not clearly define who falls under this definition, then it may lead to legal uncertainty as to who has the obligation to make data available for secondary use under Articles 33(1) and 44 of the Proposal, which in turn, might undermine the rights to privacy and data protection of data subjects. Moreover, the definition is inconsistent with Article 3(8) of the Proposal, which also refers to the social security sector, currently not encompassed by the same definition provided by Article 2(2)(y) of the Proposal. The EDPB and the EDPS are thus of the view that, for the sake of legal certainty, it is important to clarify such concept.

45. Article 2(2)(z) of the Proposal defines the **'data user'** as "*a natural or legal person who has lawful access to personalpersonalpersonal or non-personal electronic health data for secondary use*". In this regard, the EDPB and the EDPS consider that its relationship with the definition of 'data recipient' under Article 2(2)(k) of the Proposal, as well as the definition of 'recipient' in the GDPR is unclear. Such lack of clarity also applies to the interplay of this definition with the notion of 'data user' in the DGA. In addition, the EDPB and the EDPS refer to the recommendation made in paragraph 37 of this Opinion on the inclusion of EUIs in this definition. Finally, the EDPS and the EDPB believe that rather than stating that a legal person has lawful access to personal electronic health data it would be more appropriate referring to whether and under which conditions this access can be performed or not.

5 PRIMARY USE OF ELECTRONIC HEALTH DATA (CHAPTER II)

46. The EDPB and the EDPS note that, with regards to the primary use of electronic health data, as provided in the Proposal, a balance has to be achieved between the facilitation of availability of electronic records, both at national, EU or international level, and the impact on the individuals' rights and freedoms in general as well as GDPR rights. The EDPB and the EDPS consider that, in order to achieve this goal, the following aspects of the Proposal should be taken into account by the co-legislator.

47. To begin with, the EDPB and the EDPS note that Article 3 of the Proposal refers to rights of natural persons in relation to primary use of their personal electronic health data[18]. The EDPB and the EDPS hold major concerns regarding the interplay of such newly introduced rights with the ones provided

[18] For instance as for the new data subject's right to restrict access of health professionals to all or part of their electronic health data established by Article 3(9) of the Proposal, it is not clear if the rules and specific safeguards to be established by Member States law according to the same provisions shall respect the rules provided for by Article 18 (2) e (3) of the GDPR concerning the right to restriction of data processing.

in Articles 15-22 GDPR. In particular, the EDPB and the EDPS are concerned regarding the overlap of the rights envisaged in the Proposal with the ones provided for in the GDPR and the risk of legal uncertainty that this may bring vis-a-vis the data subjects. Therefore, the EDPB and the EDPS, for the sake of legal certainty, urge the co-legislature to clarify the relationship between these rights and to ensure they do not (directly or indirectly) limit the scope of individuals' rights under EU data protection legislation.

48. Article 3 of the Proposal introduces the right of immediate access and the right to give access or request the transmission of data to recipients of their choice, as well as the right to restrict access of health professionals to all or part of their electronic health data and to obtain information on the healthcare providers and health professionals that have accessed their electronic health data in the context of healthcare. As stated in Recital 1 of the Proposal, "[*t]he aim of this Regulation is to establish the European Health Data Space ('EHDS') in order to improve access to and control by natural persons over their personal electronic health data in the context of healthcare (primary use of electronic health data) […]*". Recital 6 of the Proposal explains that the EHDS builds upon the GDPR rights of the data subjects and further develops them while supporting a coherent application of those rights as applied to electronic health data.

49. Within this context, the EDPB and the EDPS underline that, at the moment of drafting of this Opinion, no data protection impact assessment [19] has been conducted on the Proposal. As a result, an assessment on how the envisaged changes may the data subject's rights and freedoms as well as the accompanying risk have not taken place.

50. Furthermore, the EDPB and the EDPS welcome that fact that the Proposal makes reference to GDPR rights (e.g. the right of access free of charge, and the right to obtain a copy of the data)[20]. However, the EDPB and the EDPS note that the description of the rights as provided in the Proposal is not consistent with the one of the GDPR. As mentioned above, this may lead to legal uncertainty vis-a-vis the data subjects who may not be able to distinguish between the two types of rights. To this purpose, and in order to avoid complexities of practical implementation, the EDPB and the EDPS urge the co-legislator to ensure legal clarity on the interplay between the data subject's rights introduced by the Proposal and the general provisions contained in the GDPR on data subject's rights.

51. This is even more relevant to ensure that data subjects with limited ability to access and use digital services are not forced to rely on third parties to exercise their fundamental rights and, consequently, are not obliged to expose their privacy and personal data to other natural persons to be able to request access to their data, as per Article 3(5)(b) of the Proposal.

52. The EDPB and the EDPS note that the representation of a data subject when exercising their data protection rights must meet certain requirements of legal certainty. The concept of authorisation introduced by Article 3(5) of the Proposal about general proxy services of access might not be

[19] The Proposal is for this matter accompanied by a Commission Staff Working Document Impact Assessment Report (doc. 8751/22 ADD 3, of 6 May 2022), which only has a general overview of three policy options on the impact on fundamental rights. This does not constitute a DPIA in the meaning of GDPR, what would be indispensable to have a thorough analysis of the risk assessment that a processing of special categories of data in a very large scale would entail and provide for the necessary mitigating measures and safeguards.
[20] See, for example, Articles 15 (1) and (3) GDPR, in what regards the existence of the right of access and the right to obtain a copy of the data, and Article 12(5) GDPR that provides for the rights be exercised free of charge.

sufficient to ensure that the data subjects was not coerced in any way to provide access to their data on their behalf to other natural persons of their choice[21].

53. Furthermore, the EDPB and the EDPS highlight that such broad concept of authorisation without any safeguards opens the door to a possible abusive use of the right of access to electronic health data. Indeed, the requirement for a representative to be a natural person only does not necessarily prevent the access to the data by private companies. Therefore, in order to prevent such possible abuse, the EDPB and the EDPS recommend to establish additional safeguards accompanying such authorisation mechanism.

54. With regards to the right to rectification provided in Article 3(7) of the Proposal, the EDPB and the EDPS note that it is not clear from the Proposal who will be responsible for ensuring the rectification of the data. This is problematic, taking into account that within this context there are multiple sources and recipients of personal data, at national level, but also at EU and even at international level. The EPDB and the EDPS highlight that, according to the GDPR, such obligation falls upon the data controller. However, since, in this context, there are several controllers contributing with electronic health data to be made available, the EDPB and the EDPS call the co-legislators to clarify in the Proposal how compliance with the right to rectification will be ensured in practice.

55. The EDPB and the EDPS note that Article 3(8) of the Proposal provides that natural persons shall have the right to give access to or request a data holder from the health or social security sector to transmit their electronic health data to a data recipient of their choice from the health or social security sector, immediately, free of charge and without hindrance form the data holder or from manufacturers of the systems used by that holder. In this regard, the EDPB and the EDPS underline that the data recipient needs to be properly identified by the system, including demonstrating that the entity receiving the data belongs to the health or social security sectors.

56. Moreover, the EDPB and the EDPS consider that, in line with the self-determination of the data subject, when deciding to which data recipient his/her electronic health data will be made available in accordance with Article 3(8) of the Proposal, the latter should ensure that the data subject could also decide which data is to be transmitted, in the same line as what the Proposal envisages in Article 3(9) of the Proposal. In particular, the EPDB and the EDPS highlight that the Proposal should provide for the possibility that only necessary data for the purpose at stake are transmitted, by requiring the adoption of technical measures of privacy by design, in order to comply with the principle of data minimisation.

57. Lastly, the EDPB and the EDPS note that, while Article 3(8) of the Proposal introduces a new right of the data subject to transmit their electronic health data to a data recipient of choice, it does not establish a corresponding explicit obligation for the data holder to do so. Since Article 9(1) GDPR, in principle, does not allow for the processing of personal data concerning health, as well as genetic data, unless one of the exemptions of Article 9(2) GDPR applies, the EDPB and the EPDS recommend the co-legislator to align Article 3(8) of the Proposal with Articles 6 GDPR and 9(2) GDPR as well as to clarify

[21] It should be taken into account that in some Member States this could only be done legally via notary, regardless of whether the person gaining access is a legal guardian or not. It is important to recall that the reason for the intervention of a notary has to do with the need to ensure a freely given indication of data subjects' wishes.

the interplay of this provision with the possible further conditions, including limitations, with regard to the processing of health or genetic data that Member States may have maintained or introduced under Article 9(4) GDPR.

58. The EDPB and the EDPS welcome the provision of Article 3(10) of the Proposal, as this guarantees that the data subjects have effective control over their personal data, enabling them to identify potential unlawful access to their health data. Nevertheless, the EDPB and the EDPS consider that it is not clear whether the right to obtain information is by means of an automatic notification procedure whenever there is access to the data, or only possible upon request. The EDPB and the EDPS consider that the first option is the most adequate solution to empower the data subject. Therefore, the EDPB and the EDPS recommend that this is something that should be taken into account the co-legislators and thus be clarified accordingly.

59. With respect to Article 4(1) of the Proposal, the EDPB and the EPDS note that health professionals shall a) have access to electronic health data of natural persons under their treatment, irrespective of the Member State of affiliation and the Member States of treatment and b) ensure that the personal electronic health data of the natural persons treated are updated with information related to the health services provided. In this regard, since the EDPB and the EDPS note that access to personal electronic health data may have been already addressed and regulated at national level, recommend that the co-legislators clarify the relationship between this provision and the national laws which already regulate this matter.

60. First, concerning Article 4(1) of the Proposal, the EDPB and the EDPS highlight that Article 9(1) GDPR, in principle, does not allow for the processing of personal data concerning health as well as genetic data, unless one of the exemptions of Article 9(2) GDPR apply. Therefore, the EDPB and the EPDS recommend that Article 4(1) of the Proposal be aligned with Article 9 (2)(h) GDPR.

61. Second, the EDPB and the EDPS consider that this provision is not in line with the GDPR principles of data minimisation and purpose limitation, since access is not granted only when necessary and on a need-to-know basis. Therefore, and in order to provide adequate safeguards to the data subjects, the EDPB and the EDPS recommend to introduce that this access shall take place on a need-to-know basis only.

62. Third, the EDPB and the EDPS highlight that the concept of “health professional” encompasses a great variety of professions of distinct nature and requiring different kinds of involvement, decision-making and responsibilities (e.g. doctors, nurses, lab and imagery technicians, nutritionists, physiotherapists, psychologists, pharmaceutics). Therefore, the EDPB and the EDPS recommend that not all health data be made available to all health professionals indiscriminately but only to those for which access is deemed necessary in order to perform a specific task. Against this background, the EDPB and the EDPS highlight the importance of the necessity and proportionality principles in this context. The EDPB and the EDPS note that, according to Article 4(2) of the Proposal, the Member States shall, in line with the principle of data minimisation, establish rules providing for categories of personal electronic health data required by different health professions. The EDPB and the EDPS note that the Proposal shall explicitly allocate this responsibility to the Member States, by making it mandatory. To this purpose, the EDPB and the EDPS recommend to replace the word “may” with “shall” so that it is ensured that such rules will be determined by the Member States.

63. The EDPB and the EDPS note that Article 4(3) of the Proposal states that access to at least the priority categories of electronic data referred to in Article 5 of the Proposal is made available to health professionals, without determining if all priority categories are accessed by all health professionals.

As indicated above, the EDPB and the EDPS consider that access should only be granted having regard to what is necessary for the purpose of the healthcare treatment. The EDPB and the EDPS consider that the relationship among Articles 4(2) and 4(3) of the Proposal should be further clarified in the Proposal.

64. Article 4(4) of the Proposal provides for the possibility to derogate from the restrictions of access selected by the data subject, foreseen in Article 3(9) of the Proposal, in case the access is necessary to protect the vital interest of the data subject or of another natural person. In this regard, the EDPB and the EDPS recommend the co-legislators to specify that the right of natural persons to obtain information on the access to their electronic health data by health professionals provided for in Article 3(10) include the accesses to the restricted information foreseen in Article 3(9) of the Proposal.

65. Article 7 of the Proposal requires Member States to ensure that health professionals "systematically" register the relevant health data concerning the health services provided by them to natural persons, in the electronic format in an EHR system. The EDPB and the EDPS are concerned about the reference to such systematic registration since it seems not to be in line with the GDPR principle of data minimisation. Therefore, the EDPB and the EDPS suggest amending the text of the Proposal by deleting the term 'systematically' in order to align the provision with the principle of data minimisation.

66. The EDPB and the EDPS welcome the provisions on electronic identity management contained in Article 9 of the Proposal since they consider that the secure identification and authentication of for natural persons and health professionals using electronic healthcare services or accessing personal health data is one of the core elements to protect the rights of the concerned data subjects. In this regard, the EDPB and the EDPS underline that it may be necessary to envisage different identification and authentication mechanism for health professionals depending whether their accesses are performed as professionals or in a private capacity.

67. As for the establishment of the Digital Health Authority, provided for in Article 10 of the Proposal, the EDPB and the EDPS are concerned by the fact that some of their tasks may overlap with those of the data protection supervisory authorities pursuant to the GDPR, especially regarding the data subject's rights and the security of the data processing. For the sake of legal certainty and to improve the readability of the legal text, the EDPB and the EDPS suggest to move the provision of Article 3(11) of the Proposal, last sentence, to Article 10 of the Proposal.

68. In relation to Article 11 of the Proposal, which establishes the right for natural and legal persons to lodge a complaint to the digital health authority, the EDPB and the EDPS consider that merely providing information on the existence of a complaint to data protection authorities is not sufficient to enable them to assess and investigate and assess any aspects of the complaint related to data protection. Therefore, the EDPB and the EDPS recommend to clarify that, if the complaint has somehow relation with data protection, even if the subject matter is related to the new rights of natural persons introduced by Article 3 of the Proposal, the digital health authority shall send a copy of the complaint to the relevant data protection supervisory authority.

69. More generally, the EDPB and the EDPS suggest introducing a mandatory consultation of and a duty of cooperation with DPAs with regard to the assessment of complaints as well as the implementation of the Proposal whenever data protection aspects are involved. Moreover, the EDPB and the EDPS underline that the data protection authorities are the only competent authorities responsible for data protection issues and therefore should remain the only point of contact for the data subject with regard to those issues, also in order to avoid any confusion for data subjects as to the modalities in which they can enforce their data protection rights.

70. Article 13 of the Proposal envisages the possibility that supplementary cross-border digital health services are provided through MyHealth@EU and that the latter is able to exchange data with other infrastructures or other services in the health, care or social security fields. The same provision requires Member States and the Commission to ensure the interoperability of MyHealth@EU with technological systems established at international level for the exchange of electronic health data.

71. The EDPB and the EDPS note that such possibilities are presented in broad terms and it is rather unclear in which circumstances and under which conditions the electronic health data can be shared with participants in third countries. In light of the safeguards required by Chapter V of the GDPR for international data transfers, the EDPB and the EDPS recommend the co-legislators to clarify that the compliance check to be performed by the Commission with regard to the national contact point of the third country or of the system established at an international level shall also cover the fulfilment of the requirements of Chapter V of the GDPR, before establishing via an implementing act that such national contact point or system is compliant with the requirements of MyHealth@EU for the purposes of the electronic health data exchange.

6 EHR SYSTEMS AND WELLNESS APPLICATIONS (CHAPTER III)

72. Chapter III of the Proposal focuses on implementing a mandatory self-certification scheme for EHR systems, where such systems must comply with the essential requirements related to interoperability and security laid down in Annex II of the Proposal. As highlighted in the explanatory memorandum, "*this approach is required to ensure that electronic health records are compatible between each system and allow easy transmission of electronic health data between them*". The EDPB and the EDPS welcome that, pursuant to Articles 15 and 17 of the Proposal, EHR systems must be subject to a prior conformity assessment procedure before these can be placed on the market or otherwise put into service in the EU.

73. However, the EDPB and the EDPS note that some of the essential requirements laid down in Annex II of the Proposal refer to aspects related to the protection of personal data, such as those addressing the implementation of the rights of natural persons, as set out in Chapter II of the Proposal, or the secure processing of electronic health data[22]. Moreover, the common specifications to be adopted by the Commission, by means of implementing acts, in respect of the essential requirements set out in Annex II, pursuant to Article 23(3) of the Proposal, may cover elements concerning data protection, such as requirements related to data quality including completeness and accuracy of electronic health data as well as requirements and principles related to security, confidentiality, integrity, patient safety and protection of electronic health data[23].

74. Firstly, the EDPB and the EDPS emphasize that compliance of EHR systems with the essential requirements related to interoperability and security laid down in Annex II of the Proposal, does not necessarily mean that the processing operations underlying their functioning are lawful per se, since further requirements resulting from the EU data protection law may need to be complied with by the controller. However, while the EDPB and the EDPS understand that the aforementioned essential

[22] See for instance points 1.3 and the security requirements listed in point 3 of Annex II, such as points 3.1. on the prevention of unauthorized access; 3.2. on identification and authentication mechanisms; 3.3. on access control mechanisms; 3.4. on logging mechanisms for data accesses and 3.5. on health professionals' access restriction mechanisms.

[23] See Article 23(3) (c) and (e) of the Proposal as well as Article 10(2)(h) of the Proposal.

requirements and common specifications are not directly linked with EU data protection law, some of them may have a significant impact upon relevant aspects for the protection of personal data of the concerned data subjects. In this regard, the EDPB and the EDPS note that the aforementioned requirements do not seem to duly take into account the principles of data minimization and data protection by design as key aspects to take into consideration when designing an EHR system in order to adequately safeguard the interest and rights of data subjects with regards to data protection and privacy. Moreover, the requirements related to retention periods and access rights in point 3.8 of Annex II of the Proposal do not take into account the specific purpose of the data processing operations, as a key element to consider to design the storage features of an EHR systems, alongside "the origins and categories of electronic health data".

75. Taking into consideration the risks posed by the provisions on the mandatory availability, cross-border sharing, access and further uses of electronic health data contained in EHR systems and the impact on the individuals concerned, the EDPB and the EDPS are of the view that, in order to strengthen the protection of individuals and their confidence in these systems, it would be most adequate to introduce a third-party conformity assessment procedure for EHR systems[24], by involving notified bodied in the assessment of the measures, including technical solutions, taken by the manufacturer to comply with the interoperability and security requirements set out in Annex II of the Proposal. In this regard, the EDPB and the EDPS positively note that this issue shall be subject to a specific assessment in the context of the evaluation and review of the Proposal carried out by the Commission after 5 years from its entry into force.

76. Moreover, the EDPB and the EDPS recommend amending the Proposal so as to clarify the relationship between the mandatory self-certification scheme for EHR systems and data protection requirements. In addition, it should be pointed out that, whenever the common specifications referred to in Article 23 of the Proposal have an impact on data protection requirements of EHR systems, the implementing acts to be adopted by the Commission pursuant to Article 23 of the Proposal should be subject to a consultation of both the EDPS and EDPB in accordance with Article 42(2) EUDPR. The same considerations apply to the voluntary labelling of wellness application which equally rely on the essential requirements laid down in Annex II of the Proposal and the common specifications referred to in Article 23 of the Proposal.

77. With regards to the handling of risks posed by EHR systems and of serious incidents, as well as the implementation of corrective actions, under Article 29 of the Proposal, the EDPB and the EDPS recommend that a duty of information to and cooperation with the DPAs, where relevant, be established. Indeed, it is not clear if the reference to the risk to "other aspects of public interest protection" among the risks that may be presented by an EHR system, thus entailing the intervention of the market surveillance authority, may include the protection of personal data. In addition, it cannot be excluded that a serious incident involving an EHR system[25] originates from malfunctions or deteriorations in the characteristics or performance of an EHR system, which also affect the protection of personal data.

[24] See for instance the third-party conformity assessment procedure provided for by the Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

[25] See the definition set out in Article 2(2)(q) of the Proposal.

78. The EDPB and the EDPS in principle welcome Article 31 of the Proposal on the voluntary labelling of wellness applications, since this can ensure transparency for the users of wellness applications regarding their key features, thereby supporting users in their choice of reliable wellness applications. However, Articles 31 and 32 of the Proposal only address wellness applications' interoperability with EHR systems and establish a mechanism of voluntary compliance limited to the interoperability and security requirements laid down in Annex II of the Proposal, with a view to ensuring that wellness applications are able to transmit electronic health data to EHR systems.

79. In this regard, the EDPB and the EDPS emphasize that the label accompanying wellness applications pursuant to Article 31 of the Proposal does not necessarily mean that the processing operations underlying the functioning of those application are lawful per se and can be deployed by the user as such. Further requirements resulting from the EU data protection law will need to be complied with by the controller. The EDPB and the EDPB recommend that this be clarified in the Proposal, even in a recital. Recital 35 of the Proposal states that "*users of wellness applications, such as mobile applications, should be informed about the capacity of such applications to be connected and to supply data to EHR systems or to national electronic health solutions, in cases where data produced by wellness applications is useful for healthcare purposes*". However, the conditions under which such wellness applications may lawfully be connected and supply personal data to EHR systems (or to national electronic health solutions) under the data protection legislation are not specified in the Proposal. What seems clear from the list of the minimum categories of electronic data for secondary use, set out in in Article 33 of the Proposal, is that indirectly - once uploaded in an EHR system[26] - or directly - insofar as they are collected and/or processed by entities falling under the definition of data holders pursuant to Article 2(2)(y) of the Proposal[27] - personal data produced by wellness applications falls under these categories and then are subject to data holders' obligation of making them available for secondary use in accordance with the provisions of Chapter IV of the Proposal.

80. Mandatory availability of electronic heath data generated by medical devices, wellness applications or other digital health applications for secondary use must be assessed against the rapid technological developments in mobile and wearable technology and the increasing popularity of 'quantified self' apps and devices, that allow people to register all kinds of aspects about their personality, mind, body, behavioural patterns and whereabouts. Clearly these types of data processing deserve significant attention, since it is not easy to recognize as the processing of health data by the concerned data subjects. However, at the same time this brings real privacy risks, especially in the case where such data are processed for additional purposes and/or combined with other data or transferred to third parties. These types of data processing may create specific risks, including the risk of unequal or unfair treatment based on data about a person's assumed or actual health status derived, for example through profiling, of very intimate details concerning his/her private life, irrespective of whether these conclusions concerning his/her health status are accurate or not. In fact, those risks may also be linked to the reliability and accuracy of data generated by medical devices, wellness applications or other digital health applications. Against this background, the EDPB and the EDPS acknowledge that Article 33(3) attempts at delimiting which data generated by medical devices, wellness applications or other digital health applications shall be made available for secondary uses. However, the EDPB and the EDPS underline that it is still unclear either what kind of data fall under this category or who would assess its validity and quality once inserted by individuals in their own EHR pursuant to Articles 3(6)

[26] See Article 3(6) and 33(1)(a) of the Proposal.
[27] See Article 33(1)(f) and (n) of the Proposal.

and 33(1)(a) of the Proposal or made directly available by data holders pursuant to Article 33(1)(f) and (n) of the Proposal.

81. In this regard, the EDPB and the EDPS recommend excluding from the scope of Chapter IV of Proposal wellness applications and other digital applications. Should these data be maintained in the scope of Chapter IV, the EDPB and the EDPS stress that users have to remain free to decide if and which of their personal data generated by wellness application and other digital applications - regardless of the fact that they have been uploaded in their own EHRs - shall be shared with other recipients and further processed for secondary uses. Therefore, the EDPB and the EDPS recommend to amend the Proposal so as to ensure that data subjects are properly informed about their possible choices with regards to the potential further uses of their electronic health data including those generated by wellness and other digital applications. Secondly, the specific conditions for the further processing of such personal data must be clearly determined in accordance with the data protection legislation and suitable mechanisms must be established to ensure that the will of the data subjects with regard to the further processing of their personal health data generated by wellness and other digital applications are respected.

7 SECONDARY USE OF ELECTRONIC HEALTH DATA (CHAPTER IV)

82. The EDPB and the EDPS acknowledge that Chapter IV of the Proposal aims to facilitate the secondary use of electronic health data and welcome the fact that such secondary use of electronic health data may generate considerable benefits for the public good. However, the EDPB and the EPDS consider that such further processing activities are not without risks for rights and freedoms of data subjects.

83. The EDPB and the EDPS take note that, in line with Recital 37 of the Proposal, the "(...) *Regulation provides the legal basis in accordance with Articles 9(2)(g), (h) and (j) of the Regulation (EU) 2016/679 for the secondary use of health data, establishing the safeguards for processing, in terms of lawful purposes, trusted governance for providing access to health data (through health data access bodies) and processing in a secure environment, as well as modalities for data processing, set out in the data permit*." Against this background, the same Recital provides that the data applicant will demonstrate a legal basis pursuant to Article 6 GDPR, based on which a request for access to data could be made in the light of the Proposal, while this not being necessarily reflected in the operative part of the Proposal. On the other hand, the EDPB and the EDPS note that Article 34(1) of the Proposal provides a list of purposes for which electronic health data can be processed for secondary use, which include, but are not limited to, the purpose of scientific research related to health or care sectors.

84. In this regard, the EDPB and the EDPS put forward three main concerns.

85. **First**, the EDPB and the EDPS note a lack of proper delineation of the purposes listed under Article 34 (1) of the Proposal for which electronic health data may be further processed, and in particular express concern with regards to Articles 34(1)(f) and (g) of the Proposal, which possibly encompass <u>any</u> form of 'development and innovation activities for products or services contributing to public health or social security' or 'training, testing and evaluation of algorithms, including in medical devices, AI systems and digital health applications, contributing to public health or social security'. The EDPB and the EDPS strongly recommend for the Proposal to further delineate these purposes and circumscribe when there is a sufficient connection with public health and/or social security, in order to achieve a balance adequately taking into account the objectives pursued by the Proposal and the protection of personal data of the data subjects affected by the processing.

86. **Second**, in the light of the observations made above and despite the wording contained in Recital 37 of the Proposal, the EDPB and the EDPS consider that the Proposal requires further improvements to ensure compliance with Article 9 GDPR.

87. Indeed, the purposes for which electronic health data may be processed for secondary use under Article 34(1) of the Proposal contain several types of secondary use, which would fall under different categories of grounds for exception foreseen in Article 9(2) GDPR. However, the EDPB and the EDPS consider that this is not reflected in the criteria according to which the health data access bodies should assess and decide on data applications (Article 45 of the Proposal) in order to issue a data access permit (Article 46 of the Proposal). The EDPB and the EDPS, to this end, highlight that the criteria provided for in this regard by Article 46 of the Proposal are restricted to the provisions and principles of this Proposal and lack clarity as to the way in which such provisions relate to the principles and provisions of the GDPR, and in particular to Article 9(2) GDPR.

88. In addition to what mentioned above, the EDPB and the EDPS seek for specific clarification on how and in which cases Article 9(2)(j) GDPR would be applicable in cases of processing health data for 'purposes in the public interest, scientific or historical research purposes or statistical purposes' (based on Union law or MS law) and 'appropriate safeguards' as required under Article 89(1) GDPR.

89. **Third**, the EDPB and the EDPS consider how this exception, construed by means of Union law, to Article 9(2) GDPR, may be reconciled with Article 9(4) GDPR and the possibility for Member State law to introduce further conditions, including limitations with regard to the processing of genetic data, biometric data or data concerning health. In this regard, the EDPB and the EDPS consider that the Proposal could clarify how the exception to Article 9(1) GDPR, stemming from the Proposal but as yet not being explicitly specified in any of the provisions of the Proposal, intend to reconcile with all different national Member States' laws.

90. As a result**, the EDPB and the EDPS call for the Proposal to ensure full compatibility with Article 9(2) GDPR and in particular with regards to its application to the purposes listed in Article 34(1)(f) and (g) of the Proposal**. Moreover, the EDPB and the EDPS also recommend to amend Article 46 of the Proposal accordingly, in order to properly integrate and reflect the differences in the goals and requirements for the secondary use of electronic health data.

91. With regard to the **minimum categories of electronic health data for secondary use**, the EDPB and the EDPS note that, under Article 33(1) of the Proposal, a legal obligation is construed, according to which data holders, by means of Union Law, shall make available specific categories of electronic health data for secondary use. The EDPB and the EDPS note that Article 41(1) of the Proposal indicates that this (new) legal obligation complements any other legal obligation (already) foreseen in other Union law or national legislation implementing Union law. As indicated in Recital 37 of the Proposal, the EDPB and the EDPS note that Article 33(1) of the Proposal would serve as legal ground under Article 6(1)(c) GDPR and would also provide for an exception to the prohibition in Article 9(1) GDPR for the data holder to process (thus make available and provide) personal electronic health data. In this regard, while the EDPB and the EDPS acknowledge that such legal obligation for data holders – in principle - fits into the system of the GDPR, may result in legal uncertainty.

92. In this regard, Article 33(5) of the Proposal provides that "[*w]here the consent of the natural person is required by national law, health data access bodies shall rely on the obligations laid down in this Chapter to provide access to electronic health data"*. The EDPB and the EDPS firstly consider that the type of 'consent-requirements' in national law the provision refers to are unclear. In particular, **the EDPB and the EDPS underline the lack of clarity as to what step in the procedure foreseen in the**

Proposal with regards to secondary use of electronic health data may the health data access bodies disregard such requirements set out in national law, in particular when falling under Article 9(4) GDPR. Moreover, the EDPB and the EDPS recommend further clarification and specification in relation to Article 46(6)(f) of the Proposal, which provides for health data access body to possibly introduce 'specific conditions in the data permit granted'.

93. Article 36 of the Proposal provides for the **establishment of health data access bodies**. In this regard, the EDPB and the EDPS highlight that the responsibility of the health data access body to assess the legal ground proposed by the data user will require availability of proper legal expertise in the health data access body. The EDPB and the EDPS note that, as yet, this is not explicitly stated in Article 36 of the Proposal. However, the EDPB and the EDPS underline that the assessment of the legal basis by the health data access body may – always – be scrutinized and - when necessary - overturned by the relevant DPA. To this end, the EDPB and the EDPS call for specific clarity as to the interplay between the role of the health data access body and the respective DPA in the context of any data protection related issue.

94. The need to clarify the relationship between the Proposal and Member States legislation is further exemplified in the context of **applications for data permits in the context of cross-border access to personal electronic health data for secondary use** (section 4, Articles 52-54 of the Proposal). The EDPB and the EDPS note that, while the Proposal aims to facilitate of cross-border secondary use, by establishing 'national contact points' and a cross-border infrastructure (HealthData@EU), data users will possibly still need to apply to the respective health data access bodies in each of the Member States. Indeed, the EDPB and the EDPS understand that Article 45(3) of the Proposal only provides for limited coordination between the health data access bodies involved, in order to obtain a data permit. However, the EDPB and the EDPS consider that the Proposal does not offer adequate clarification as to the specific national law that will be applied in the context of cross-border data permits (the one of the respective health data access body or the one of the data applicant), including the legal basis that will need to identified (by the data applicant) and assessed (by the health data access body). Lastly, in this regard, it should also be noted that both on the part of the health data access body and on the part of the data user there may be (significant) gaps in expertise to overcome problems in identifying and appreciating differences in (requirements to be met as laid down in) Member State's laws pertaining to (such) a legal basis.

95. The EDPB and the EDPS note that Article 38(2) of the Proposal provides that health data access bodies shall not be obliged to provide the specific information under Article 14 GDPR to each natural person concerning the use of their data for projects subject to a data permit. In this regard, the EDPB and the EDPS consider that the exemption introduced may lead to unintended consequences for the fundamental rights and freedoms of data subjects, due to the lack of concrete conditions under which such an exemption would be applicable.

96. Furthermore, the EDPB and the EDPS recall the importance of transparency obligations towards data subjects and urge the co-legislator to identify specific situations to ensure that such provision may not be systematically relied upon by health data access bodies. Therefore, the EDPB and the EDPS recommend to modify the provision accordingly taking into account that the requirements set out in Article 14 GDPR may not be systematically overruled without adequate and relevant assessment and justification as to the need to rely on such exemption[28]. Should the restriction of the right to

[28] See also paragraph 25 above.

information be maintained, the EDPB and the EDPS highlight to the co-legislators the need to consider the conditions provided for in Article 23 GDPR.

97. Article 40 of the Proposal defines and provides for the data altruism in the context of health. In this regard, the EDPB and the EDPS consider the provision unclear, particularly with regards to the interplay with the respective provision introduced by the DGA. To this end, the EDPB and the EDPS recommend to clarify the provision accordingly.

98. The EDPB and the EDPS positively note the provision of Article 44(3) of the Proposal, which states that where health data access bodies have to provide access to data in pseudonymised format, the data users shall not re-identify the electronic health data provided in such format (the information to reverse pseudonymisation shall only be available to the health data access bodies). Moreover, the EDPB and the EDPS welcome the fact that the same provision of the Proposal states that in case of failure on behalf of the data user to respect the health data access body's measures used to ensure pseudonymisation, the former shall be subject to appropriate safeguards.

99. Lastly, Article 48 of the Proposal provides that, by derogation from Article 46 of the Proposal, a data permit shall not be required to access the electronic health data under the same Article by public sector bodies and Union institutions, bodies, offices and agencies. The EDPB and the EDPS consider that a permit should also be required, in order to enable verification that all relevant requirements, including lawfulness and necessity, have been complied with. Moreover, the EDPB and EDPS consider such a requirement important to promote transparency, as the Proposal envisages that health data access bodies shall shall provide general public information on all the data permits issued pursuant to Article 46.

8 ADDITIONAL ACTIONS (CHAPTER V)

8.1 Storage of personal electronic health data in the EU and compliance of international data transfers with Chapter V GDPR

100. Chapter V of the Proposal aims to put forward other measures to promote capacity building by the Member States to accompany the development of the EHDS. In addition, this Chapter regulates the international access and transfer *non-personal* electronic (health) data, as well as well international access and transfer of *personal* electronic health data.

101. As regards international access and transfer of *personal* electronic health data, Article 63 of the Proposal specifies that Member States 'may maintain or introduce further conditions, including limitations, in accordance with and under the conditions of Article 9(4) of the Regulation (EU) 2016/679'.

102. **First,** the EDPB and the EDPS would like to recall that, in its judgment in *Digital Rights Ireland*, the CJEU considered that the absence of a requirement to retain the data within the EU meant that "*[...] it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security [...] is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals*

with regard to the processing of personal data"[29]. In other words, the CJEU explicitly held, in the case at hand, that control of compliance with the requirements of protection and security by an independent supervisory authority cannot be fully ensured in the absence of a requirement to retain the data in question within the EU. The failure to require data to be retained in the EU was among the considerations which led the CJEU to conclude that the EU legislature had exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter[30].

103. The need to impose a requirement to store personal data in the EU in certain specific cases was then confirmed and complemented in the *Tele 2* judgment in which the CJEU considered that *'Given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period*' (emphasis added)[31]. Again, the CJEU underlined that in order to guarantee the necessary level of security and protection of the data in question, the relevant legislation **must** require data to be retained in the EU.

104. The EDPB and the EDPS consider that the findings made by the Court in these two landmark judgments are also relevant in the context of the Proposal, as it will apply to (i) the processing of a large quantity of personal data, (ii) that are of a highly sensitive nature and (iii) for which there is no objective element to conclude that the risk of unlawful access is inferior than that identified in the context of the judgments referred to above.[32] In particular, the EDPB and the EDPS stress that the finding of the Court is all the more likely to apply to the data at hand considering that health data is likely to be considered as even more sensitive than telecommunications data (i.e. the data at hand in the two judgments referred to above).

105. In this context, the EDPB and the EDPS share the concerns of the Court regarding the need to mitigate the risks of unlawful access and ineffective supervision when it comes to certain types of data and certain types of processing operations. In particular, the EDPB and the EDPS note that in case the

---

[29] Judgment of the Court (Grand Chamber), 8 April 2014, *Digital Rights Ireland Ltd*, joined Cases C-293/12 and C-594/12; para 68. See also the Opinion of Advocate General Cruz Villalón delivered on 12 December 2013 in the same case at para 78 and 79, noting that the absence provision that lays down the requirement to 'store the data to be retained in the territory of a Member State, under the jurisdiction of a Member State', 'increases the risk of use which is incompatible with the requirements resulting from the right to privacy' and 'considerably increases the risk that such data may be accessible or disclosed in infringement of that legislation'.

[30] Judgment of the Court (Grand Chamber), 8 April 2014, *Digital Rights Ireland Ltd*, joined Cases C-293/12 and C-594/12; para 69.

[31] Judgment of the Court (Grand Chamber) of 21 December 2016, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, joined Cases C-203/15 and C-698/15, para 122. See also the opinion of Advocate General Saugmandsgaard Øe delivered on 19 July 2016, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, joined Cases C-203/15 and C-698/15, para 239 to 241.

[32] The EDPB and the EDPS note that this risk of unlawful access is such that it has actually conducted the Commission to dedicate a specific provision on the matter for what concerns non-personal data (Article 62 of the Proposal).

processing infrastructure is located in non-EU/EEA Member States, EU data protection supervisory authority's control over compliance with EU data protection rules might not always be fully ensured.

106. In addition, the EDPB and the EPDS note that the Commission recently proposed data storage requirements in another context: Article 17(1)(c) of the recent Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union indeed provides that 'sensitive non-classified information should be stored and processed in the EU'[33]. More generally, the EDPB and the EDPS note that EU law already provides several examples of pieces of existing legislation imposing to store personal data in the EU and that usually go even further by also restricting transfers[34]. The EDPB and the EDPS therefore conclude that EU law requires, in certain specific situations, to impose that the data be stored in the EU in order to mitigate the risk of unlawful access and to ensure effective supervision.

107. **Second,** the EDPB and the EDPS note that Article 62 of the Proposal, on international access and transfers of non-personal electronic heath data, refers in several instances to non-personal electronic health data 'held in the EU', which would seem to indicate a general assumption that this category of data would have to be stored in the EU. The EDPS and EDPB consider that the same approach should be adopted for personal data falling within the scope of the Proposal, as it would seem difficult to justify having a requirement to store non-personal electronic health data in the EU but not having the same requirement for personal electronic health data.

108. **Third,** The EDPB and the EDPS wish to clarify in this context that an obligation to store personal data in the EU does not preclude transfers of personal electronic health data to third countries or international organisations. Indeed, it is possible to reconcile a general requirement to store personal data in the EU with specific transfers being allowed compliance with Chapter V GDPR (e.g. in the context of scientific research, disbursement of care, international cooperation). Consequently, the EDPB and EDPS consider that the obligation to store the data in the EU would be proportionate and would not go beyond what is necessary to achieve the objective pursued, which is to lay down an additional safeguard with the view to mitigate the risk of unlawful access and ineffective supervision over the data concerned, given its highly sensitive nature.

---

[33] Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union
COM/2022/119 final; https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52022PC0119

[34] See e.g. Article 6(8) of Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime: 'The storage, processing and analysis of PNR data by the PIU shall be carried out exclusively within a secure location or locations within the territory of the Member States'; Article 3 of Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation); Article 41 of Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011; Article 39 of Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II).

109. **Fourth,** the EDPB and the EDPS also note that Article 63 of the Proposal provides that Member States may maintain or introduce further conditions, including limitations, in accordance with and under the conditions of Article 9(4) GDPR. Such limitations imposed at a national level may include an obligation to store data in the EU. The EDPB and the EDPS draw attention to the fact that such an obligation already applies in several Member States and consider it likely that several Member States would impose or continue to impose similar obligations if the matter is not harmonised at EU level.

110. In view of the above, the EDPB and the EDPS therefore consider it essential to avoid an inconsistent and fragmented approach throughout the EU that would lead to different degrees of protection of data subjects, which would be at odds with one of the key objectives of the GDPR.[35] Therefore, the EDPB and the EDPS consider that additional obligations including storage of personal electronic health data within the EU should be as far as possible addressed at EU level i.e. in the Proposal, in order to ensure a uniform high level of protection for data subjects across the EU, as well as to preserve the proper functioning of the internal market, in line with Article 114 TFEU on which the Proposal is based.

111. For all the above reasons and having due regard to the highly sensitive nature of the personal data at hand, **the EDPB and the EDPS consider that Article 63 of the Proposal should impose on controllers and processors established in the EU processing personal electronic health data within the scope of the Proposal an obligation to store this data in the EU.** As explained above, such a requirement to store personal electronic health data in the EU should be **without prejudice to the possibility to transfer personal electronic health data in compliance with Chapter V GDPR**.[36] The EDPB and the EDPS also recommend to recall in the preamble that controllers and processors processing personal electronic health data remain subject to Article 48 GDPR on transfers or disclosures not authorised by EU law and should comply with this provision in case of access request stemming from a third country[37].

8.2 Procurement and Union funding

112. The EDPB and the EDPS note that Article 60 of the Proposal addresses the question of additional requirements for public procurement and Union funding. The EDPB and the EDPS consider that the above recommendations (on data storage in the EU and compliance with Chapter 5 and in particular Article 48 GDPR) would be best operationalised if they were embedded at an early stage when procuring [38] or funding services provided by controllers and processors established in the EU processing personal electronic health data.

---

[35] See recital 53 GDPR relating to Article 9(4) GDPR: 'However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.'

[36] And provided that the other conditions of the GDPR are complied with, in particular Article 6 GDPR on the obligation for the processing to be lawful.

[37] Article 48 GDPR: 'Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.'

[38] In this respect, Recital 78 of the GDPR provides that 'the principles of data protection by design and by default should also be taken into consideration in the context of public tenders'. Furthermore, Recital 77 of Directive 2014/24/EU on public procurement provides that 'when drawing up technical specifications, contracting authorities should take into account requirements ensuing from Union law in the field of data protection law, in particular in relation to the design of the processing of personal data (data protection by design)'.

113. Therefore, **the EDPB and the EDPS recommend that Article 60 of the Proposal also refers, as a condition to procure or fund services provided by controllers and processors established in the EU processing personal electronic health data, that such controllers and processors (i) will store this data in the EU and (ii) have duly demonstrated that they are not subject to third country legislations conflicting with EU data protection rules.**

8.3 National contact points of a third country or systems established at international level

114. The EDPB and the EDPS note that Articles 13(3) and 52(5) of the Proposal provide for the possibility for national contact points of a third country or systems established at an international level to be recognised compliant with the requirements of respectively MyHealth@EU and HealthData@EU. The EDPB and the EDPS recall that transfers stemming from the connection to and use of MyHealth@EU and HealthData@EU should comply with Chapter V GDPR.

115. The EDPB and the EDPS note that Articles 13(3) and 52(5) of the Proposal provide for the possibility for national contact points of a third country or systems established at an international level to be recognised compliant with the requirements of respectively MyHealth@EU and HealthData@EU. The EDPB and the EDPS recall that transfers stemming from the connection to and use of MyHealth@EU and HealthData@EU should comply with Chapter V GDPR.

116. In particular, the EDPB and the EDPS note that both Article 13(3) and Article 52(5) of the Proposal refer to compliance checks to be carried out by the Commission before issuing the implementing act establishing that a national contact point of a third country or a system established at an international level is compliant with the requirements of MyHealth@EU or HealthData@EU. The EDPB and the EDPS also note that Recital 26 of the Proposal, relating to MyHealth@EU, refers to the need for these checks to ensure 'compliance of the national contact point with the technical specifications, data protection rules and other requirements [...]'. **In this respect, the EDPB and the EDPS recommend clarifying directly in both Article 13(3) and Article 52(5) of the Proposal that the compliance checks should ensure that Chapter V GDPR will be complied with once the national contact point of a third country or a system established at an international level is connected to MyHealth@EU or HealthData@EU.**

9 EUROPEAN GOVERNANCE AND COORDINATION (CHAPTER VI)

117. The EDPB and the EDPS note that Article 64 of the Proposal establishes the EHDS Board**,** a coordination body which aims to facilitate cooperation and the exchange of information among Member States. The EDPB and the EDPS note that the EHDS Board will be composed of representatives of digital health authorities and health data access bodies of all Member States and that **the EDHS Board will be chaired by the Commission.** The EDPB and the EDPS note that, in line with the Proposal, the EDPB and the EDPS representatives may be invited to the meetings when data protection issues are discussed. **The EDPB and the EDPS consider that their representatives should be permanent members of the EHDS Board (thus not only potentially invited) and should participate to all discussions on personal data protection issues**, in order to ensure a consistent interpretation and application of the provisions introduced by the Proposal with regard to the provisions of the GDPR.

118. Moreover, Article 65(1) of the Proposal defines the tasks of the EHDS Board on the primary use of electronic health data. The EDPB and the EDPS notice that the Commission will be able to issue written

contributions and to exchange best practices on matters related to the implementation of the Proposal, in particular on the provisions set out in Chapters II and III of the Proposal (Article 65(1) (b) (i)) and on any aspect of the primary use of electronic health data (Article 65.1 (b) (iii)). Since Chapter II of the Proposal provides data protection rights similar to the GDPR (see point 28), the EDPB and the EDPS consider that the EHDS Board should not be able to issue written contributions related to data protection rights issues. Otherwise, **the EDPB and the EDPS underline that the Proposal risks introducing a divergence in the interpretation or the application of data protection rights** determined by the EDPB and the EDPS. Moreover, the EDPB and the EDPS note that this provision will create legal uncertainty, which will also be in contradiction with the Proposal's goals to improve the functioning of the internal market by laying **down a uniform legal framework** (Recital 1 of the Proposal). In addition, Article 65(2) of the Proposal specifies the EHDS Board tasks relating to the secondary use of electronic health data. The EDPB and the EDPS reiterate their warning regarding the competences of the EHDS Board to publish written contributions on issues related to data protection rights regarding secondary use of electronic health data.

119. Furthermore, according to Articles 65(1) (d) and 65(2)(d) of the Proposal, the EDPB and the EDPS note that the EHDS Board will be able to share information concerning risks and data protection incidents related to primary and secondary use of electronic health data together with information regarding their handling. **Once again, the EDPB and the EDPS stress that the Proposal risks introducing a divergence between the EDPB, the EDPS and the EHDS Board regarding the identification or the handling of data breaches**, since the EDHS Board will be able to share information on how data protection incidents could be handled. Besides, there is unclarity as to the recipients of the information the EHDS board will share. More generally, the EDPB and the EDPS recommend the co-legislator to specify the interplay between the EDPB, the EDPS and the EHDS Board on the data protection issues, which should remain the exclusive competence of the data protection authorities.

120. With respect to the same chapter, the EDPB and the EDPS note that Article 66 of the Proposal states that the Commission shall establish two subgroups dealing with joint controllership for the cross-border infrastructures MyHealth@EU and HealthData@EU (Articles 12 and 52 of the Proposal). **The EDPB and the EDPS note that the scope of the tasks of the joint controllership groups are not clearly defined, and that they may overlap with the EHDS Board tasks** under Article 65 of the Proposal. More generally, the EDPB and the EDPS recommend that the interplay between the different bodies, groups and organizations mentioned in the Proposal shall be clearly defined.

121. In addition, the EDPB and the EDPS note some inconsistencies between the subgroups' tasks and the power of the Commission to adopt implemented or delegated acts on the same topics. For instance, according to Article 52(13) of the Proposal, the Commission may set out the requirements, the technical specifications, the IT architecture of HealthData@EU through implementing acts, whereas one of the two sub-groups will also make decisions concerning the development and operation of the same infrastructure. **Therefore, the EDPB and the EDPS recommend that the interplay between the Commission and these sub-groups is clarified.**

10 DELEGATION AND COMMITTEE (CHAPTER VII)

122. Chapter VII of the Proposal allows the Commission to adopt delegated acts on several concrete aspects regulated by the Proposal. In this regard, the EDPB and EDPS note that, regardless of the Member States' involvement in the decision making, the power to decide to modify or extend some of the essential issues addressed by the Proposal still leaves the Commission with a considerable margin for

manoeuvre to modify or extend the scope of the same Proposal in a way that could impact data protection rights and the Member States' exclusive competence to define their national health policies.

123. In particular, the EDPB and the EDPS consider that Articles 5(2) and 33(7) of the Proposal raise concerns, since the Commission is empowered to amend the list of priority categories of electronic health data to be accessed and exchanged across Member States for primary use as well as the list of electronic health data, subject to the mandatory availability and access by third parties for secondary use. As any modification of such categories of personal data, notably special categories of data, might require a re-evaluation of the risks to the fundamental rights and interests of the concerned individuals, these issues amounts to substantive matters that should be considered as essential elements, pursuant to Article 290 of the TFEU.

124. Therefore, the EDPB and the EDPS consider that such matters should not be excluded from the legislative level, where any restriction of fundamental rights should be clearly provided to achieve the indispensable foreseeability of the legal instrument while only more detailed data fields (sub-categories of data) falling under the already defined categories of data set out in Articles 5(1) and 33(1) of the Proposal should be added through the adoption of delegated acts.

125. Moreover, the EDPB and the EDPS note that the criteria envisaged by Article 5(2)(b) of the Proposal to guide the Commission in deciding the priority categories of electronic health data to be added to the list established in Article 5(1) of the Proposal seem vague and should be further delimited[39].

126. Finally, even though Article 67(4) of the Proposal states that the Commission shall consult experts designated by each Member State, which may involve some expertise in data protection matters, the EDPB and the EDPS recommend to introduce a clear reference to Article 42 of the EUDPR to make clear that the EDPS and EDPB shall be consulted as appropriate when such delegated acts are proposed.

11 MISCELLANEOUS (CHAPTER VIII)

127. The EDPB and EDPS note that Chapter VIII of the Proposal allocates the responsibility for establishing penalties applicable to infringements of the Regulation on EU Member States. The EDPB and the EDPS consider that this could potentially lead to significant legal uncertainties with respect to the proper enforcement of the rules established by the Proposal in different Member States, due to the different determination of penalties' size, which could be with significantly different minimum and maximum amount enforced from one to another Member State. In this regard, the EDPB and the EDPS note that harmonised rules on penalties should be established in order to ensure fair and safe enforcement, especially in the context of cross-border cases.

128. Lastly, the EDPB and the EDPS note that, in line with previous comments on the self-certification of EHR systems, the periods for evaluation and review established under Article 70 of the Proposal are too long to ensure the proper implementation in time.

[39] The criteria refer to the "category used in a significant number of EHR systems used in Member States" according to the most recent information.

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

[1] For example, it is not clear whether manufacturers would fall within this categorisation.