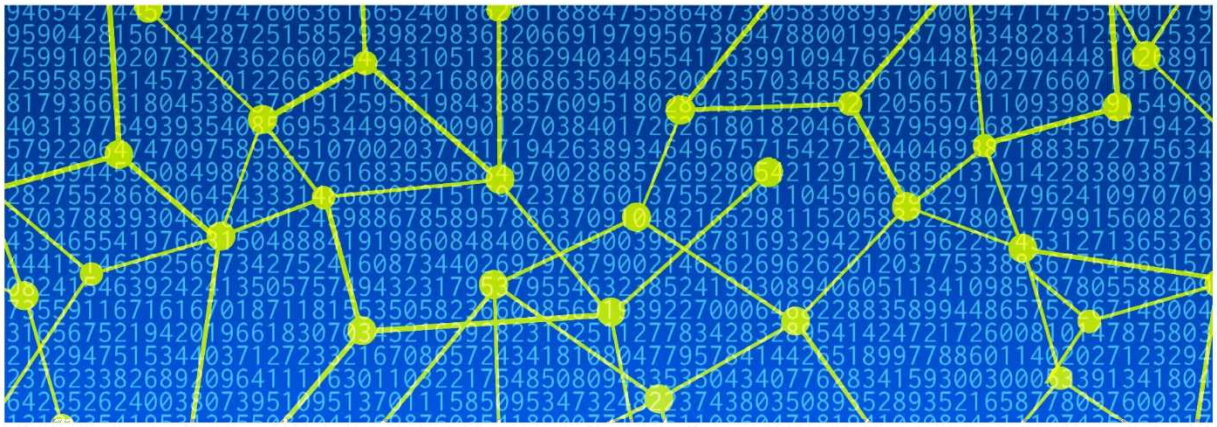

EUROPEAN DATA PROTECTION SUPERVISOR

Preliminary Opinion 8/2020 on the European Health Data Space

EDPS

17 November 2020

The European Data Protection Supervisor (EDPS) is an independent EU authority, responsible under Article 52(2) of Regulation 2018/1725 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies', and under Article 52(3)'…for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under article 58(3)(c) of Regulation 2018/1725, the EDPS shall have the power 'to issue on his or her own initiative or on request, opinions to Union institutions and bodies and to the public on any issue related to the protection of personal data'.

Wojciech Wiewiorówski was appointed Supervisor on 5 December 2019 for a term of five years.

Executive Summary

On 19 February 2020, the European Commission presented its Communication on "A European strategy for data". This communication envisages the creation of a common space in the area of health, namely the European Health Data Space ('EHDS'), presented as an essential tool for the prevention, detection and cure of diseases as well as for the taking of evidence-based decisions and to enhance effectiveness, accessibility and sustainability of the healthcare systems.

Whereas the EDPS strongly supports the objectives of promoting health-data exchange and fostering medical research, it underlines the necessity for data protection safeguards to be defined at the outset of the creation of the EHDS. Thus, with this preliminary opinion the EDPS highlights the essential elements that should be considered in the development of the EHDS from the data protection perspective.

The EDPS calls for the establishment of a thought-through legal basis for the processing operations under the EHDS in line with Article 6(1) GDPR and also recalls that such processing must comply with Article 9 GDPR for the processing of special categories of data.

Moreover, the EDPS highlights that due to the sensitivity of the data to be processed within the EHDS, the boundaries of what constitutes a lawful processing and a compatible further processing of the data must be crystal-clear for all the stakeholders involved. Therefore, the transparency and the public availability of the information relating to the processing on the EHDS will be key to enhance public trust in the EHDS.

The EDPS also calls on the Commission to clarify the roles and responsibilities of the parties involved and to clearly identify the precise categories of data to be made available to the EHDS. Additionally, he calls on the Member States to establish mechanisms to assess the validity and quality of the sources of the data.

The EDPS underlines the importance of vesting the EHDS with a comprehensive security infrastructure, including both organisational and state-of-the-art technical security measures to protect the data fed into the EHDS. In this context, he recalls that Data Protection Impact Assessments may be a very useful tool to determine the risks of the processing operations and the mitigation measures that should be adopted.

The EDPS recommends paying special attention to the ethical use of data within the EHDS framework, for which he suggests taking into account existing ethics committees and their role in the context of national legislation.

The EDPS is convinced that the success of the EHDS will depend on the establishment of a strong data governance mechanism that provides for sufficient assurances of a lawful, responsible, ethical management anchored in EU values, including respect for fundamental rights. The governance mechanism should regulate, at least, the entities that will be allowed to make data available to the EHDS, the EHDS users, the Member States' national contact points/ permit authorities, and the role of DPAs within this context.

The EDPS is interested in policy initiatives to achieve 'digital sovereignty' and has a preference for data being processed by entities sharing European values, including privacy and data protection. Moreover, the EDPS calls on the Commission to ensure that the stakeholders taking part in the EHDS, and in particular, the controllers, do not transfer personal data unless data subjects whose personal data are transferred to a third country are afforded a level of protection essentially equivalent to that guaranteed within the European Union.

The EDPS calls on Member States to guarantee the effective implementation of the right to data portability specifically in the EHDS, together with the development of the necessary technical requirements. In this regard, he considers that a gap analysis might be required regarding the need to integrate the GDPR safeguards with other regulatory safeguards, provided e.g. by competition law or ethical guidelines.

TABLE OF CONTENTS

I. Contents

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[1],

Having regard to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC[2], in particular Articles 42(1), 57(1)(g) and 58(3)(c) thereof,

Having regard to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA[3],

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction and scope of the Opinion

1. On 19 February 2020, the European Commission ('Commission') presented its Communication on "A European strategy for data".[4] This was part of a package of documents, including a Communication on Shaping Europe's digital future[5] and a White Paper on Artificial Intelligence - A European approach to excellence and trust[6].

2. One of the key initiatives of the European strategy for data ('Data Strategy') is to create **Common European data spaces in strategic sectors and domains of public interest**, which would increase the possibilities for public authorities and business to access high quality data, boost growth and create value. More generally, the various initiatives of the Data Strategy go in line with the Commission's ambition to have the "(...) *EU at the forefront of the data-agile economy, while respecting and promoting the fundamental values that are the foundation of European societies*".[7]

3. The EDPS released its **Opinion 3/2020 on the European strategy for data** ('Opinion 3/2020') in June 2020[8], after an informal consultation on a draft version by the Commission in January 2019. Opinion 3/2020 presents the EDPS' views on the Data Strategy, and touches particularly on certain relevant concepts from a data protection perspective, including the notion of 'public good', Open Data, use of data for scientific research, data intermediaries, data altruism and international data sharing.

4. The EDPS notes that eHealth is a key area of public interest where the Commission's Data Strategy envisages the creation of a common space, namely the **European Health Data Space ('EHDS')**. In accordance with the Data Strategy, the EHDS will be essential for the prevention, detection and cure of diseases, as well as for evidence-based decisions in order to enhance effectiveness, accessibility and sustainability of the healthcare systems.[9]

5. In its recent meeting of October 2020, also the European Council welcomed *"(...) the European strategy for data, which supports the EU's global digital ambitions to build a true European competitive data economy, while ensuring European values and a high level of data security, data protection, and privacy. It stresses the need to make high-quality data more readily available and to promote and enable better sharing and pooling of data, as well as interoperability. The European Council welcomes the creation of common European data spaces in strategic sectors, and in particular invites the Commission to give priority to the health data space, which should be set up by the end of 2021."*[10]

6. **Whereas the EDPS strongly supports the objectives of promoting health-data exchange and fostering research on new preventive strategies, treatments, medicines, medical devices, it also underlines the necessity for data protection safeguards to be defined at the outset**. In the context of the Covid19 pandemic, the European Union has seen more than ever the need for the GDPR data processing principles to be fully applied. In line with the recent European Council Conclusions, **the EDPS recalls the fundamental rights to data protection and privacy,** and calls for data protection principles to be integrated in the future eHealth solutions that will soon be at the heart of all European eHealth systems. In this context, we highlight that data protection safeguards must be embedded in the core of the upcoming EHDS**,** with the aim of guaranteeing the respect of fundamental rights of individuals, including the right to privacy and to the protection of personal data of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('the Charter').

7. **The aim of this preliminary opinion is** to contribute to the Commission's work on the future EHDS, in particular through identifying of the essential elements that should be considered in the development of the EHDS from the data protection perspective. T**his preliminary opinion should be read in conjunction with other relevant EDPS Opinions**, including the Opinion on the European Strategy for Data[11], the preliminary Opinion on scientific research[12], the Opinion on Open Data[13], the Opinion on the European Commission's White Paper on Artificial Intelligence[14] and the EDPS Opinion on the proposal for a recast of the Public Sector Information (PSI) re-use Directive.[15] It is worth underlining that this preliminary opinion is without prejudice to any future EDPS opinion that may be issued in accordance with Article 42 of Regulation (EU) 2018/1725 on the related forthcoming legislative proposals of the Commission.

2. The European Union's eHealth initiatives

8. The EDPS acknowledges that **multiple EU initiatives on eHealth already exist**, *inter alia*, the Directive 2011/24/EU on patients' rights in cross-border healthcare ('the Patients' Rights Directive'), the European Reference Networks ('ERNs'), the Clinical Patient Management System ('CPMS'), the eHealth Network and the eHealth Digital System Infrastructure ('eHDSI'). The main features of these initiatives are as follows:

9. **Directive 2011/24/EU on patients' rights** in cross-border healthcare[16] guarantees the right of individuals to access healthcare in any of the EU Member States and sets out the conditions under which EU patients may be reimbursed for healthcare costs in their home country. In particular, the Patient's Rights Directive aims at ensuring an easier access to information on available healthcare in other EU Member States, together with alternative healthcare options and/or specialised treatments abroad. The Directive creates a network of National Contact Points providing information on cross-border healthcare, develops EU rules on an essential list of elements to be included in cross- border medical prescriptions and fosters the development of the European Reference Network (ERN)[17] of medical expertise, in order to broaden the cooperation between EU Member State in eHealth. The same Directive also creates the **eHealth Network**[18], a voluntary network of Member States' competent authorities responsible for eHealth. Moreover, in order to facilitate interoperability, the eHealth network, assisted by the Commission, developed an IT tool, the so-called **eHealth Digital Service Infrastructure** ('eHDSI')[19], with the scope of exchanging health data under the Connecting Europe Facility programme, also developed by the Commission.

10. The Directive not only enables patients to be reimbursed for treatment in other EU Member States, but also enhances access to information on healthcare, thus increasing the options for treatment, including rare diseases, through the (currently 24) **ERNs**[20], who work on different thematic issues. These are virtual networks involving healthcare providers across Europe and aim at dealing with complex or rare diseases, which require highly specialised treatment and a concentration of knowledge and resources. Therefore, the ERNs enable patients' reimbursement for treatment in other EU Member States and enhance access to information on healthcare, thus increasing the options for treatment, including rare diseases. The Commission's role is to create the framework for the ERNs and to provide technical networking facilities.

11. As the Directive also entrusts the Commission with the role of supporting the ERN's establishment, functioning and evaluation through specific implementing measures, the Commission has developed the **CPMS platform**[21]. This aims at facilitating remote collaboration by health professionals in the ERNs for the diagnosis and treatment of patients with rare or low prevalence complex diseases or conditions across national borders and fostering scientific research of such diseases or conditions. The CPMS processes sensitive data concerning patients who suffer from rare or low prevalence complex diseases to facilitate patients' diagnosis and treatment, for scientific research, clinical or health policy purposes and for contacting potential participants for scientific research initiatives. For all these three cases, the patient signs a specific consent.

3. The Common European Health Data Space

3.1 Context and legal basis

12. Pursuant to the Commission's Data Strategy, **the objective of the proposed European Health Data Space (EHDS) is to improve access to and quality of healthcare, by helping competent authorities in firstly, taking evidence-based policy decisions and secondly, supporting scientific research.** According to this strategy, the Commission intends to achieve this goal by deploying data infrastructures, tools and computing capacity[22] for the EHDS, namely a platform that will allow certain data to be processed for the benefit of society. The EHDS will thus foster the development and interconnection of

the abovementioned eHealth initiatives by enhancing research and innovation and facilitating policy-making decisions and regulatory activities of Member States in the area of public health.

13. The EDPS acknowledges that **a common EHDS will be an essential tool to improve the accessibility, effectiveness and sustainability of the health systems as well as to allow informed, evidence-based policy decisions relating to them.** Indeed, public health policy is an area where the EU can benefit from a data revolution that makes possible an increase of the quality of healthcare, while decreasing costs.

14. As the EDPS highlights in its Opinion 3/2020 on the European strategy for data, given the sensitive nature of health data, **all processing operations**, which might result from the establishment of such a common health data space **will require a robust legal basis** in line with EU data protection law. In this regard, we recall that the EU's primary legislation, and in particular, **Article 168 TFEU** sets the goal of encouraging cooperation between the Member States in the area of public health and, if necessary, lend support to their action, with the view to improve the complementarity of their health services in cross-border areas.

15. Moreover, processing operations under the EHDS will only be lawful if they are based on one or more of the six legal bases exhaustively listed in **Article 6(1) GDPR.** As the scope of the EHDS' creation is to enhance access to health data in order to allow for evidence-based policy decisions and for scientific research within the EU, we do not consider Article 6(1)(a) GDPR (i.e. consent of the data subject), as the most appropriate legal basis to enhance such aim. Rather, the EDPS considers that **Article 6(1)(e) GDPR may possibly be the most appropriate legal basis** for the processing of personal data in the context of the functioning of the EHDS, as the platform's main purpose will be to serve the public interest and the processing should be done in the exercise of official authority vested in the controller.

16. **In addition, it is recalled that health data are a "special category of data"** to which the GDPR affords special protection through the establishment of certain safeguards for its processing. In this regard, the EDPS considers that **Article 9(2)(i) GDPR**, which allows processing of sensitive data for reasons of public interest, could be considered as a possible legal basis for the processing operations carried out within the EHDS in relation to the specific purpose of taking **evidence-based policy decisions by competent authorities**. In addition, **Article 9(2)(j) GDPR** could be a possible legal basis for processing operations involving health data when the processing is necessary **for scientific research purposes.** Such processing must also be in accordance with Article 89(1) based on Union or Member State law which requires the processing to be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. In this context, the EDPS would like to draw the attention to the recently adopted EDPB Guidelines on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak.[23] These also touch upon the essential data protection requirements applicable to this processing, in particular legality, transparency, necessity and proportionality, as well as integrity and confidentiality.

17. The EDPS, in its preliminary opinion on Scientific Research[24], has already called for a **need for further harmonisation** of data protection rules applicable to health data among the Member States. As also echoed in the Data Strategy, "*the landscape of digital health services remains fragmented, especially when provided cross-border*".[25] In order to

overcome such fragmentation in terms of harmonisation, the EDPS welcomes the Commission's initiative to facilitate the establishment, in accordance with Article 40 of the GDPR, of a **Code of Conduct** for processing of personal data in health sector.[26] Furthermore, **in the context of processing of data for scientific research in health**, we consider that EU-wide Codes of Conduct in the respective research areas could be an effective enabler of cross-border exchange of data that **would contribute to providing further clarity and building trust** from patients and individuals into the system.

18. Closely linked to the lawfulness of the processing, is the principle of **purpose limitation**. In this regard, the EDPS notes that the purpose(s) for which the health data may be processed within the EHDS must be clearly established prior to the processing. **The boundaries of what constitutes a lawful processing and a compatible further processing of the data must be crystal-clear for all the stakeholders involved**. The processing in the context of the future EHDS must comply with the requirements of Articles 5(1)(b) GDPR (purpose limitation), Article 6(4) GDPR (compatibility test), as well as Article 89(1) GDPR (safeguards and derogations relating to processing for scientific purposes), read in the light Article (50) GDPR. The Article 29 WP Opinion 3/2013[27] provides useful guidance on the implementation of the purpose limitation principle, as well as on the appropriate use of the various legal bases for personal data processing and remains largely relevant also under the GDPR.

19. Where the legal basis for further processing of data within the EHDS is consent, the technical means implemented therein should be granular enough to allow for the respect of the will of the data subjects, for example, when they have expressed a consent limited to certain situations such as usage by public sector bodies or specific research types. This being noted, the EDPS considers that forthcoming legislation should indeed determine specific **conditions for further processing of personal data** and establish mechanisms to ensure that the data made available for secondary use are not unlawfully harvested or used for purposes that were not foreseen initially, are disproportionate or lack an adequate legal basis. Moreover, the conditions should not be discriminatory and should follow a necessity and proportionality approach. Finally, **to strengthen the transparency of the personal data processing on the EHDS, the conditions for further processing of personal data should be publicly available.**

20. Moreover, the EDPS notes that **lawful further processing of data**, including when measures such as anonymisation are applied, **might not solve all ethical problems**, such as for example those relating to personal objections to certain private sector stakeholders (e.g. pharmaceutical, insurance, etc.) having access to the individual's sensitive personal data[28]. In this regard, it is recalled that anonymization also requires a lawful legal basis within Articles 6 and 9 of the GDPR, and must comply with the requirements for a compatible further processing[29]. Therefore, in the context of the EHDS, the Commission should ensure that the future legal framework to be established also takes into account such circumstances and that data subjects are properly informed about the potential further processing of their data.

21. The EDPS calls on the Commission to clarify the roles and responsibilities of the parties involved, in particular as regards the **identification of controllers within the context of the EHDS**, before whom individuals are able to exercise their data protection rights. In this regard, we recall that, pursuant to Article 24 GDPR, the public sector body vested with the role of controller in each Member State would be accountable for the processing, i.e. it would need to demonstrate compliance with the GDPR. In particular, that public body

would be responsible for the implementation of appropriate technical and organisational measures aimed to ensure the respect of the data protection rights of individuals.

22. The EDPS recommends the Commission to clearly **identify the precise categories of data to be made available to the EHDS.** In particular, the decision on the categories of data should be defined by the legislator at a level of granularity that enhances accuracy of data while still ensuring a lawful basis and the respect of the data protection principles under the GDPR. Moreover, the EDPS recalls the fundamental need for an adequate check-and-balance system (at national level) and in the context of a public interest and ethical objective.

23. As to the **sources of that data**, we are of the view that this should be a responsibility of the national Member States' contact points/permit authorities, who would assess the validity and quality of the type of data submitted by the parties sharing such data. Following the necessity and proportionality principles, the EDPS believes that the data made available to the EHDS should as a general rule be made anonymised and aggregated. If this were not possible due to the nature of the data at stake and the purpose of the processing, this should at least be pseudonymised.

24. In this regard, and as in Opinion 3/2020 on the European Strategy for Data, the EDPS once again underlines the essential importance of **the application of data protection safeguards together with organisational and technical measures within the EHDS development and governance.** In line with Article 5 of the GDPR, the processing of personal data within the EHDS will need to respect the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality. In this context, we also recall the fundamental importance of the requirements of data protection by design and by default, which need to be fully applied by all actors involved, in full compliance with the GDPR.[30]

25. As an example, to implement data minimisation, safeguards should consider, as appropriate and as far they have reached the state-of-the art maturity, the use in context of privacy enhancing technologies, including those enabling to perform operations on encrypted data without having access to the data in clear or performing calculations on distributed data without having access to all data sources or enabling reliable statistical calculations on data where noise has been injected.

26. Moreover, the EDPS underlines that the EHDS must have a **comprehensive security policy, organisation and infrastructure**, including both **organisational and state-of-the-art technical security measures** to protect the sensitive data fed into the EHDS. In particular, we recall the obligations of Article 32 GDPR and recommend, given also the nature of the health data as "special category of data" based on Article 9 GDPR, the use of effective encryption as a baseline requirement, together with the establishment of strict authentication procedures and access restrictions based on data classification and use on a case-by-case basis, and the adoption of further measures of enhanced security for the storage space and intra-European data flows. Moreover, accurate logging and auditing should be performed in order to ensure the security of the data contained in the platform and the accountability of its use.

27. As in Opinion 3/2020, the EDPS also recalls the essential role of **Data Protection Impact Assessments ('DPIAs')**, as the use of data within the meaning of public interest involves large-scale processing, combining data from various sources and involving special categories of data. In these cases, and as such processing is likely to result in a high risk,

data controllers have the obligation to conduct DPIAs in accordance with Article 35 of the GDPR. Moreover, the EDPS once again recommends, whenever possible, making public the results of such assessments, as an enhancing measure of trust and transparency. The measures adopted because of the risks assessed in the DPIA should follow the principle of data protection by design and by default. The inception phase of the EHDS is the best suited for the implementation of such principle. In this regard, we recall the EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.[31]

28. In sum, the EDPS strongly believes that **transparency to and control by data subjects are key**. This can only be achieved through a common understanding as to what the main actors and third parties can and cannot do within the EHDS together with precise modalities as to what data and how data can be accessed. **Exhaustive agreements on the use of the EHDS and clear rules on the data's management** should be foreseen in the legislative framework at stake. Moreover, the EDPS highlights that, in line with Article 42 GDPR, stakeholders participating in the EHDS may establish data protection certification mechanisms and data protection seals and marks, for the purpose of demonstrating compliance with the GDPR and enhancing trust.

29. In addition, **the EDPS calls for special attention to the essential need of the ethical use of such data**. As also recommended in the abovementioned opinion, "[*E]thics committees can play a meaningful role in ensuring that the respect of human rights, including right to data protection, is embedded in the research project from the early planning stage. They are likely to continue to play an important role in ensuring that research projects are designed from the start with data protection principles in mind*".[32] As a result, **forthcoming legislation should also take into account existing ethics committees and their role in the context of national legislation**, while also paying particular attention to the need to determine a common understanding and general rules as to how data could be ethically processed and re-used in the context of the processing within the EHDS. However, it should also be clarified that ethics committees cannot absolve controllers from their obligations to meet their obligations under EU data protection law, to be supervised by the independent supervisory authorities set up for that purpose.

3.2 Governance

30. According to the information available at this stage, the forthcoming Commission proposal on Data Governance would establish the main principles for the governance of the future European Data Spaces, including the EHDS. These general principles would be complemented by additional mechanisms and safeguards, to be included in future sectoral legislation.

31. The EDPS is of the view that **the success of the EHDS will depend on the establishment of a strong data governance mechanism, fully compliant with the GDPR that provides for sufficient assurances of a lawful, responsible, ethical management anchored in EU values, including respect for fundamental rights**. In this regard, the EDPS considers 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 the society as a whole.[33]

32. Moreover, in order to establish an effective and solid governance, the EDPS is of the view that any legislative act providing for such platform must clearly **identify the main actors involved in the processing** of personal data within it and define their role as data controller, processor or joint controller. In line with the relevant data protection legislation, their roles

and responsibilities should be assessed thoroughly, particularly to guarantee the respect of data subject's rights and to consequently ensure a high level of trust by EU citizens. In this regard, **the EDPS suggests that the future governance framework for the EHDS should include at least the following elements.**

33. **Entities making data available to the EHDS**: these would be responsible for the primary collection and quality of the data and could make data available to the EHDS through specifically identified Member States' national contact points;

34. **EHDS users** (i.e. research organisations, patients and users' associations, institutions, but also private companies, start-ups etc.). In this regard, the EDPS recommends that such actors be required to demonstrate specific objectives with scientific and research relevance with evident purposes of public interest, to be conducted in an ethical framework;

35. **Member States' national contact points/ permit authorities**: in most EU Member States, researchers may only obtain data by approaching the relevant databases individually, this being a burdensome and complex process. The EDPS is of the view that the EHDS legislative proposal should provide for Member States to have a single national contact point or permit authority, which would act as coordinator between the requests to have access to specific data and the databases relevant for their research initiatives. These bodies could also carry out an assessment of the objectives' requirements with scientific and research relevance under the law and would thus not only facilitate the access to health data in a cross-border context, but would also ensure an effective control over the entire process. We believe that such national contact points/ permit authorities could take the form of **independent new bodies**, or also existing **ethics committees, without interference with the powers of the independent data protection supervisory authorities established under EU law**.

36. In this regard, the EDPS considers fundamental for the **European Data Protection Authorities** ('DPAs') to be formally involved in the EHDS' supervision and data protection compliance. We also take note that in the context of existing data spaces, such as the French Health Data Hub, the respective DPAs already act as authorisers of access to specific data according to criteria of data protection and respect for citizens' rights.[34] The **EDPS**, as the supervisory authority for processing of personal data by EU institutions, offices, bodies and agencies, must be involved in the EHDS' supervision, given the likely central role by EUIs in the governance of the data space at hand, in coordination with national DPAs in the context of the EDPB, as appropriate.

37. **The EDPS does not support the creation of artificial geographical borders, but has a preference for data being processed by entities sharing European values, including privacy and data protection**. The EDPS is interested in policy initiatives to achieve 'digital sovereignty', where data generated in Europe is converted into value for European companies and individuals, and processed in accordance with EU rules and regulations.[35]

38. In this regard, **the EDPS calls on the Commission to ensure that the controllers taking part in the EHDS ('data exporters') ensure full compliance with the rules of the GDPR,** as interpreted by the CJUE **in particular in *Schrems II***.[36] This may involve, where necessary, the adoption by the data exporters of measures (having technical, contractual and organisational nature) supplementing the appropriate safeguards entered into with the controllers or processors in the third country of destination of the data. To do so, data exporters should conduct a transfer impact assessment in compliance with the steps described in the EDPB Recommendations on measures that supplement transfers tools to

ensure compliance with the EU level of protection of personal data.[37] In case the implemented measures, considered sufficient on the basis of the data transfer impact assessment, no longer ensure adequate protection of the personal data transferred, the data exporter shall suspend or prohibit such transfer to the third country. Consequently, **the Commission** should **ensure that the stakeholders taking part in the EHDS, and in particular, the controllers, do not transfer personal** data unless data subjects whose personal data are transferred to a third country are afforded a level of protection essentially equivalent to that guaranteed within the European Union.

39. Lastly, the **European Commission** would be responsible for the EHDS' creation, governance and development of technical and organisational measures. We also consider that **EU Agencies** whose mission is closely related to the processing of health data (such as EMA and ECDC) should be able to directly connect and access the EHDS, in order to simplify their work and performance of their tasks. The EDPS thus recommends to ensure that their roles and responsibilities, including the conditions under which these may access the EHDS, be fully clarified, also in accordance with data protection law.

3.3 The right to data portability

40. The EDPS welcomes the specific acknowledgement in the European Data Strategy of the **citizens' right to access and control their personal health data and to request their portability**[38], as well as the Commission's aim to work to solve the fragmented implementation of this right. In particular, the Commission has committed to taking measures to strengthen citizens' access to health data and portability of these data and tackle barriers to cross-border provision of digital health services and products.[39] Moreover, the Commission has committed to working in ensuring portability of the personal data within the Electronic Health Record (EHR), within and across borders, as this "*will improve access to and quality of care, cost effectiveness of care delivery and contribute to the modernisation of health systems*".[40]

41. The EDPS notes that the right to data portability is essential to enhance "control" by data subjects over their data and that the imperfect data portability mechanisms currently existing can present an obstacle to the effectiveness of this right.[41] The right to data portability i**s a right that may only enforced upon the data subject's request** and entails the possibility for a data subject to receive a subset of the personal data processed by a data controller concerning him or her, and to store those data for further personal use. Such storage can be on a private device or on a private cloud, without necessarily transmitting the data to another data controller.[42]

42. The EDPS also notes that, in line with the GDPR, the right to data portability may not be applicable in the context of a task carried out in the public interest. As a result, the EDPS invites the Commission to ensure in its legislative proposal that **Member States guarantee the application of this right together with the development of the necessary technical requirements specifically in the EHDS** that allow and effective use of this right by data subjects.

43. The EDPS highlights that **there are still gaps that should be addressed in the future legislation on the EHDS in order to make the right to data portability effective**. As indicated by the EDPB, **the right to data portability covers data provided knowingly and actively by the data subject as well as the personal data generated by his or her activity**.[43] In this regard, the EDPB has clarified that the outcome of an assessment regarding the health of a user (i.e. derived data such as medical diagnosis etc.) cannot in

itself be considered as "provided by" the data subject and thus will not be within scope of this right. This is so, even if such data may be part of a profile kept by a data controller and are inferred or derived from the analysis of data provided by the data subject.

44. Moreover, some authors have pointed to the fact that under the research exemption for the processing of special categories of data under Articles 9(2)(j); 5(1)(b); 6(4) and 89 GDPR, data subjects appear to be significantly excluded from the control over their processed health data. Therefore, in the context of the EHDS, **a gap analysis might be required regarding the need to integrate the GDPR safeguards with other regulatory safeguards,** provided e.g. by competition law or ethical guidelines.[44]

45. The EDPS recalls that pursuant to Article 20(1) of the GDPR **data subjects have the right to transmit their data to another controller without any legal, technical or financial obstacles** placed by data controller in order to refrain or slow down access, transmission or reuse by the data subject or by another data controller. In this context, the EDPS calls for Member States, where appropriate, to encourage the use of open, machine-readable formats. Moreover, we highlights that in implementing the right to data portability, data controllers should assess the specific risks linked with data portability and take appropriate risks mitigation measures.

4. Conclusions and recommendations

In light of the above, the EDPS makes the following recommendations:

46. **Supports the initiative to create a common European Health Data Space** and acknowledges its key role to improve access to and quality of healthcare, by helping competent authorities in taking evidence-based policy decisions and by supporting scientific research. However, the EDPS calls for the adoption of **necessary data protection safeguards in parallel to the works towards the creation of the EHDS**.

47. Recalls that all processing operations resulting from the EHDS' establishment will require **a robust legal basis in line with EU data protection law**, particularly Article 6(1) GDPR and Article 9 GDPR for the processing of special categories of data.

48. Considers that the forthcoming legislative initiative on the **EHDS should also aim at contributing to a mitigation of the current fragmentation of rules applicable to the processing of health data and to scientific research**, thus also aimed at guaranteeing a lawful and ethical use and re-use of the data within the EHDS.

49. Advocates for additional clarity on the **boundaries of what constitutes a lawful processing and a compatible further processing of the data for all stakeholders involved in the EHDS process**, while also strengthening the transparency of data processed by making the conditions for re-use publicly available.

50. Considers essential the setting of clear rules to the Member States for the **identification of controllers within the context of the EHDS**, before whom individuals may be able to exercise their data protection rights, in line with current legislation (GDPR and Regulation 2018/1725).

51. Requests that the **main actors involved and the categories of data processed** within the EHDS are clearly identified and considers fundamental for the **European Data Protection**

Authorities ('DPAs') to be clearly involved in its supervision and data protection compliance.

52. Calls for the adoption of a **comprehensive security infrastructure**, including both organisational and state-of-the-art technical security measures to protect the sensitive data fed into the EHDS.

53. Recalls the essential role of **Data Protection Impact Assessments** ('DPIAs'), and recommends, whenever possible, making public the results of such assessments, as an enhancing measure of trust and transparency.

54. Calls for the establishment of a **strong data governance mechanism** that providing for sufficient assurances of a lawful, responsible and ethical management of the data processed within the EHDS.

55. Has a preference **for data being processed by entities sharing European values**, including privacy and data protection.

56. **Strongly supports the achievement of data sovereignty where data generated** in Europe is converted into value for European companies and individuals, and processed in accordance with EU rules and regulations.

57. Calls on the Commission **to ensure that the stakeholders taking part in the EHDS, and in particular, the controllers, do not transfer personal data unless data subjects whose personal data are transferred to a third country are afforded a level of protection essentially equivalent to that guaranteed within the European Union.**

58. Invites the Commission to ensure in its legislative proposal that Member States **guarantee the application of the right to data portability** together with the development of the necessary technical requirements in the EHDS that allow and effective exercise of such right by data subjects.

59. Recommends performing **a gap analysis regarding the need to integrate the GDPR safeguards with other regulatory safeguards,** provided e.g. by competition law or ethical guidelines.

Brussels, 17 November 2020

Wojciech Rafał WIEWIÓROWSKI

(e-signed)

Notes

[1] OJ L 119, 4.5.2016, p. 1.
[2] OJ L 295, 21.11.2018, p. 39.
[3] OJ L 119, 4.5.2016, p. 89.
[4] COM 2020 66 final https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.
[5] COM(2020) 67 final, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europedigital-future_en
[6] COM(2020) 65 final, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trustartificial-intelligence_en
[7] COM (2020) 66 final https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN, p.2.
[8] EDPS Opinion 3/2020 on the European Strategy for Data https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf .
[9] COMM 2020 66 final https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf, p. 22.
[10] See https://data.consilium.europa.eu/doc/document/ST-13-2020-INIT/en/pdf .
[11] EDPS Opinion 3/2020 on the European Strategy for Data https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf .
[12] EDPS Preliminary Opinion on data protection and scientific research https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf .
[13] EDPS Opinion on the 'Open-Data Package' of the European Commission including a Proposal for a Directive amending Directive 2003/98/EC on re-use of public sector information (PSI), a Communication on Open Data and Commission Decision 2011/833/EU on the reuse of Commission documents, https://edps.europa.eu/sites/edp/files/publication/12-04-18_open_data_en.pdf .
[14] EDPS Opinion 4/2020 EDPS on the European Commission's White Paper on Artificial Intelligence– A European approach to excellence and trust https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf .
[15] EDPS Opinion 5/2018 on the proposal for a recast of the Public Sector Information (PSI) re-use Directive https://edps.europa.eu/sites/edp/files/publication/18-07-11_psi_directive_opinion_en.pdf .
[16] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare OJ L 88, 4.4.201.
[17] See https://ec.europa.eu/health/ern_en .
[18] See https://ec.europa.eu/health/ehealth/policy/network_en .
[19] See https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHDSI+GOVERNANCE . See also EDPB-EDPS Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI), https://edps.europa.eu/sites/edp/files/publication/19-07-15_edpb_edps_joint_opinion_ehealth_en.pdf .
[20] See https://ec.europa.eu/health/ern_en .
[21] See https://ec.europa.eu/health/sites/health/files/ern/docs/cpms_ps_en.pdf .
[22] See Commissions' Data Strategy, page 30
[23] EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, 21.04.2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf.
[24] EDPS preliminary Opinion on Data Protection and Scientific Research https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.
[25] Reference and link!
[26] EDPS Opinion 3/2020 on the European Strategy for Data https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf, p. 29
[27] Article Working Party 29 Opinion 03/2013 on purpose limitation https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
[28]See Peek N. and Rodrigues Pereira P., "Three controversies in health data science", 07 March 2018, Springer https://link.springer.com/article/10.1007/s41060-018-0109-y.
[29] See WP29 Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[30] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 13.11.2019, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf .
[31] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 13.11.2019, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf .
[32] EDPS preliminary Opinion on Data Protection and Scientific Research https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf p. 25.
[33] EDPS Opinion 3/2020 on the European Strategy for Data https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf .
[34] See https://www.health-data-hub.fr/faq .
[35] See https://edps.europa.eu/sites/edp/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf .
[36] Judgement of the Court (Grand Chamber) of 16 July 2020 in case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems.
[37] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en.
[38]COM (2020) 66 final, p.29
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN
[39]COM (2020) 66 final,
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN
[40] COM (2020) 66 final,
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN.
[41] See https://www.digitaleurope.org/wp/wp-content/uploads/2020/05/WEB28APR2020_The-role-of-a-health-Data-Space-in-a-pandemic_slides-Ioana.pdf
[42] Article 29 WP Guidelines on the right to data portability, 13.12.2016, as revised and adopted on 5 April 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 and endorsed by the EDPB on 25 May 2018.
[43] Idem.
[44] Schneider G., Health Data Pools under European Policy and Data Protection Law: Research as a New Efficiency Defence?, 11 (2020) JIPITEC 49 para 1, available at https://www.jipitec.eu/issues/jipitec-11-1-2020/5082/schneider_pdf.pdf .