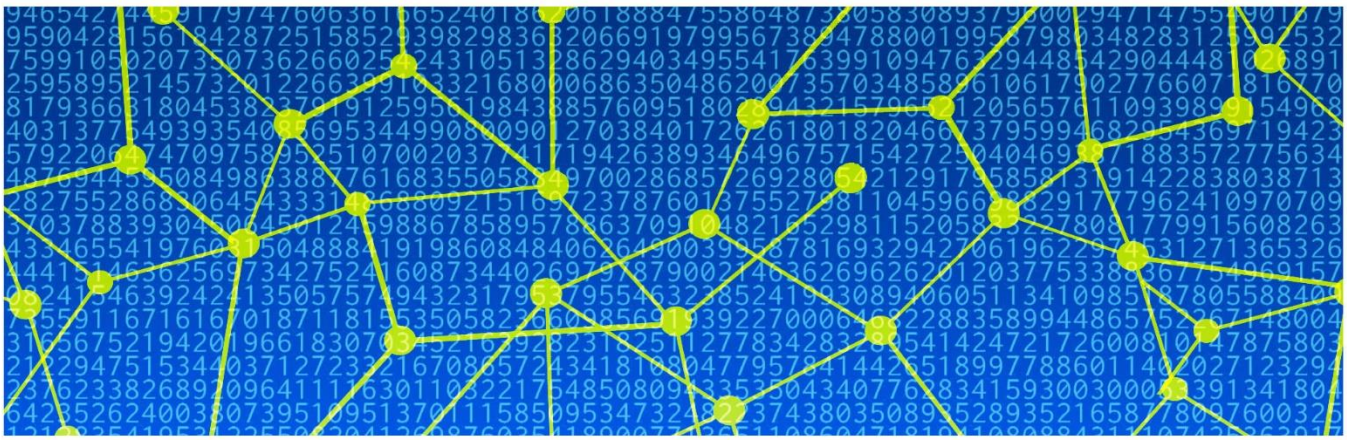

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 3/2020

on the European strategy for data

EDPS

16 June 2020

Executive Summary

The European Commission published on 19 February 2020 a Communication "A European strategy for data". It is part of a wider package of strategic documents, including also a Communication on Shaping Europe's digital future and a White Paper on Artificial Intelligence - A European approach to excellence and trust.

The aim of the Data Strategy is to create a single European data space and thus make it easier for businesses and public authorities to access high-quality data to boost growth and create value. Moreover, it should "enable the EU to become the most attractive, most secure and most dynamic data-agile economy in the world". A key element of the Data Strategy is the development of common European data spaces in strategic economic sectors and domains of public interest, such as the common European health data space.

This Opinion presents the EDPS view on the Data Strategy as a whole, as well as on certain specific aspects, such as the notion of "public good", Open Data, use of data for scientific research, data intermediaries, data altruism, international data sharing and others.

The EDPS understands the growing importance of data for the economy and society and supports the wider strategic objectives of the EU, such as the development of the Digital Single Market and the EU's digital sovereignty. At the same time, he recalls that "big data comes with big responsibility" and therefore appropriate data protection safeguards must be in place.

In this regard, the EDPS applauds the Commission's commitment to ensure that European fundamental rights and values, including the right to the protection of personal data, underpin all aspects of the Data Strategy and its implementation. In particular, he appreciates the assurance that the Strategy would be developed in full compliance with the General Data Protection Regulation, which provides a solid basis, also by virtue of its technologically-neutral approach.

The EDPS underlines that one of the objectives of the Data Strategy should be to prove the viability and sustainability of an alternative data economy model - open, fair and democratic. Unlike the current predominant business model, characterised by unprecedented concentration of data in a handful of powerful players, as well as pervasive tracking, the European data space 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.

Furthermore, this Opinion takes into account the unprecedented global crisis, caused by the COVID-19 pandemic, which has affected all aspects of our life. In this context, the EDPS reiterates his position that data protection is not the problem but part of the solution. Data and technology can play an important role in the overcoming the crisis in combination with other factors, as there is no "silver bullet" for something as complex like this.

The EDPS remains at the disposal of the Commission, the Council and the European Parliament to provide further advice at the next stages of the implementation of the European strategy for data, both in terms of legal framework and of practical aspects. The comments in this Opinion are without prejudice to additional comments in the future on particular issues and/or if further information is available.

TABLE OF 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 Article 58(3)(c),

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 BACKGROUND

1. The European Commission presented on 19 February 2020 a Communication "A European strategy for data"[4]. It is part of a wider package of strategic documents, including also 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. The aim of the European strategy for data (hereinafter referred to as "the Data Strategy" or "the Strategy") is to create a single European data space and thus make it easier for businesses and public authorities to access high quality data to boost growth and create value, while reducing the carbon footprint of the EU economy. Moreover, it would play a key role in realising the Commission's ambition to "enable the EU to become the most attractive, most secure and most dynamic data-agile economy in the world".

3. The European Data Strategy has been open to public consultation. The objective of the consultation is to collect views on the Data Strategy as a whole, as well as on certain specific aspects. A similar public consultation has been launched on the White Paper on Artificial Intelligence.

4. The EDPS was informally consulted by the Commission on 29 January 2020 on the initial draft of the Data Strategy and submitted preliminary comments. The EDPS welcomes the fact that his views have been sought at an early stage of the procedure and encourages the Commission to continue with this best practice.

5. The present opinion further elaborates upon some of the informal comments and provides more targeted input in light of the public consultation. It should, in principle, be read in conjunction with other relevant opinions of the EDPS, referred throughout the document, such as the Preliminary opinion on scientific research[7], Opinion on Open Data[8], Opinion on personal

information management systems[9], and others. Furthermore, the present opinion is without prejudice to any additional comments that the EDPS could make on the basis of further available information at a later stage, including in the context of the future legislative consultations on the legal acts foreseen in the Data Strategy and the Commission Work Programme.

6. Finally, the EDPS notes the ongoing debate about the extent to which data and technology can help in the fight against COVID-19. In this context, the EDPS would like to recall his position, shared by the other supervisory authorities within the European Data Protection Board (EDPB)[10], that data protection rules do not hinder measures taken in response to the coronavirus pandemic. Data protection is not the problem, it is part of the solution. The EDPS considers that data and technology play an important role in the overcoming of the unprecedented crisis, which impacts all aspects of our life, but they are by no means a "silver bullet". Data and technology can contribute in fighting the pandemics and other similar threats only if they empower effectively the individuals and are accompanied by appropriate safeguards and other holistic measures.

2. GENERAL COMMENTS

2.1. Application of the key data protection principles

7. The EDPS welcomes the Data Strategy's commitment to ensure that **European fundamental rights and values**, including the right to the protection of personal data provided under Article 8 of the Charter of Fundamental Rights of the EU and Article 16 TFEU, are fully upheld in all the actions that will follow from the Strategy.

8. In particular, the EDPS supports the Commission's commitment to develop the Strategy in full compliance with the General Data Protection Regulation ("GDPR"). He is convinced that the **GDPR provides a solid basis**, also by virtue of its technologically-neutral approach, for the development and implementation of the Strategy.

9. The EDPS recalls that, pursuant to Article 5 of the GDPR, the processing of personal data should always respect the **principles** of lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality.

10. These principles remain fully applicable when processing personal data for the "public good" purposes. **Purpose limitation** is an essential safeguard to provide individuals with the confidence that the data they provide will not be used against them in an unexpected manner. The importance of the principle of purpose limitation is clearly demonstrated in the context of the measures which are being considered to fight against COVID-19, e.g. health data to be processed under the control of healthcare authorities as data controllers and not to be used for commercial or other incompatible purposes.

11. Equally significant are the principles of **transparency and accountability**. Transparency should be understood as an obligation to provide clear, intelligible and easily accessible information both to the citizens/the public and to data protection authorities. Furthermore, the possibility to perform independent audits on the data processing operations and to take enforcement measures, whenever necessary, are important aspects of accountability and cannot be replaced by self-regulation only.

12. In the context of the proposed future **Data Act,** the EDPS recommends to lay down requirements for producers of products, services and applications that are based on the processing of personal data or which process personal data to also comply with data protection legislation, in particular with the requirements of **data protection by design and by default**. Such an obligation should complement the existing obligations of controllers and processors under the GDPR, and could

considerably enable controllers and processors to fulfil their data protection obligations, e.g. when selecting appropriate hardware or software solutions.

13. The EDPS recalls that the adoption of the proposed **ePrivacy Regulation**[11] is crucial to protect the fundamental rights to privacy and personal data protection in the digital age. Hence, the completion of the EU's legal framework for data protection and confidentiality of communications is an important condition for the success of the Data Strategy.

14. The EDPS observes that the implementation of the Strategy will inevitably entail an increase in magnitude and seriousness of the data protection risks, including **security risks**. For instance, connected Internet of Things (IoT) devices increase the "attack surface" for cyberattacks and amplify or produce new possible adverse impacts on individuals. This problem should be addressed in the context of the review of the Directive on security of network and information systems (NIS Directive) or via a new legislative initiatives, and might also be linked to EU consumer law and policy, for instance on product safety.

2.2. Data subject rights and the role of data intermediaries

15. The EDPS welcomes the objective of the Strategy to empower the individuals to be in control of their data, *inter alia* by providing tools and means to decide at a granular level about what is done with their data ("personal data spaces"). In the same vein, the Strategy aims at enhancing the portability right of individuals under Article 20 of the GDPR.

16. An important prerequisite for individuals to be able to exercise effectively their rights as data subjects is the ability to ascertain what has done with their data and by whom, given the fact that pooling of data will facilitate access by many different actors. Therefore, the routine approach to transparency in the form of lengthy privacy notices phrased in abstract or ambivalent terms, still applied by some controllers, is contrary to the GDPR's requirements to provide information "in a concise, transparent, intelligible and easily accessible form, using clear and plain language".[12]. In this context, and especially in the light of technological developments the EDPS reminds that pursuant to Article 12(7) and (8) of the GDPR the information to data subjects could be provided with **standardised and machine readable icons** in order to offer an easily visible, intelligible and meaningful overview of the intended processing. The Commission should by 2022 determine with delegated acts how the required information would be presented with such standardised icons.

17. **Personal information management systems (PIMS)** are emerging as promising platforms to give data subjects more control over their personal data. Furthermore, some PIMS models could be seen as a driver for data portability as they can function as a centralized data infrastructure allowing the individuals to manage their personal data. The EDPS has already published an Opinion on Personal Information Management Systems[13]. Therein, the EDPS stresses the need to develop technical tools and standards that make the exercise of data subjects' rights simple (e.g. with data privacy dashboards), as important means to empower the individual to manage their data. In his Opinion on PIMS the EDPS has also pointed out in particular the requirement for such systems to be fully transparent towards users and to ensure genuine user control.

18. The EDPS notes that there are other types of **data intermediaries** such as data trusts and cooperatives, data marketplaces, data brokers, etc. In this regard, the EDPS emphasises the need of a clear distinction between the data intermediaries focussing exclusively on personal data and seeking to enhance individual agency, on the one hand, and those driven by economic incentives and aiming to support mainly Business to Business (B2B) data exchange, on the other hand.

19. The EDPS considers that intermediaries aiming to empower data subjects through technical and other tools to manage the use of their data deserve consideration, **further research and effective support**, as they contribute to a sustainable and ethical use of data, in line with the principles of the GDPR.

20. At the same time, the EDPS underlines the need of caution with regard to the role of **data brokers** that are actively engaged in the collection of huge datasets, including personal data from different sources. They tap into a variety of data sources used for data-related services, such as data that are disclosed for other unrelated purposes; data from public registers (open data), as well as data "crawled" from the Internet and social media, often in violation of data protection legislation. In this context, the EDPS notes that the activities of big data brokers are under increased scrutiny and are investigated by a number of national data protection authorities[14].

2.3. Concept of "public good"

21. The Data Strategy pays specific attention to "**availability of data for the public good**", understood in a broad sense - from healthcare and environmental protection to fight against crime. The EDPS welcomes the Commission's vision on the fostering the use of data for "public good". The EDPS recalls one of the overarching principles of the GDPR, namely that processing of personal data should be designed to serve humankind.[15]

22. The EDPS also notes that the Strategy equally refers to the notion of "**public interest**", and uses it interchangeably with the notion of "public good". "Public interest" can be a basis for lawful processing under Articles 6(1)(e) of the GDPR and can be relied on for the processing of special categories of data (e.g. data concerning health) under and 9(2)(g) and (i) of the GDPR. In line with Article 6(3) of the GDPR, the basis for processing of personal data, necessary for the performance of a task carried out in the public interest, should be laid down by EU or Member State law. Consequently, processing of personal data for "public good" corresponds to the same important objectives, expressed in the GDPR as "public interest," and should be subject to the same requirements.

23. In this context, the EDPS notes that data, in particular public sector information, could play a key role in the Digital Single Market. Furthermore, smart use of data, including its processing via Artificial Intelligence, can have a transformative effect on various sectors of economy. At the same time, the EDPS points out that the sharing of data for social and other common needs should be subject to the **appropriate data protection safeguards** in line with the principles of **necessity and proportionality**.

24. The use of data for the public good/public interest may involve large-scale processing, which combines data from a variety of sources, potentially involving special categories of data and/or personal data of vulnerable groups of data subjects. Where that is the case, such processing is likely to result in a high risk and data controllers have to conduct **data protection impact assessments** (DPIA) in accordance with Article 35 of the GDPR[16]. Moreover, the EDPS recommends, whenever possible, making public the results of such assessments, as a trust and transparency enhancing measure.

25. Any subsequent use of data, collected and/or shared for a public good/public interest function (e.g. for improving transport/mobility or tackling serious cross-border threats to health), for commercial for-profit purposes (for instance insurance, marketing, etc.) should be avoided. Such **"function creep"** might not only constitute a breach of the data protection principles under Article 5 of the GDPR, but could also undermine the trust of the citizens, which is a fundamental component of the Strategy.

26. Equally important, processing of data for the public good should **not create or reinforce situations of data oligopoly** (dependency of the public sector, SMEs, etc. on few powerful IT companies, so-called Big Tech)[17]. This is also relevant from a data protection perspective since monopolies and oligopolies create situations of users' lock-in and ultimately restrict the possibility for individuals to exercise effectively their rights.

2.4. Open Data

27. Regarding the Government to Business (G2B) data re-use envisaged in the Strategy, namely the access to and processing of data held by public authorities, as defined under the 'PSI Directive'[18], revised by Directive 2019/1024/EU (hereinafter, the **Open Data Directive**)[19], the EDPS has issued an Opinion[20],whereby he referred to the following key principles:

    (i) **transparency** and **societal participation** on the purpose of the reuse *vis-à-vis* the citizens/data subjects, as well as transparency and clear **purpose definition** between the licensor (the public authority) and the licensees;

    (ii) **data protection impact assessment** for data processing falling under Article 35(3) of the GDPR to identify the risks and the appropriate data protection safeguards addressing them, before the reuse of data takes place.

28. The EDPS remarks that, due to the technological, economic and legal specificities of each 'sector' (e.g. the processing of health data for research purposes is different than the processing of smart energy data to implement 'green business model')[21], a **'sector-by-sector' approach**, requiring *inter alia* a 'sectoral' data protection assessment, might be necessary.

29. From the information technology viewpoint, the EDPS welcomes that the Strategy aims to foster the reuse of public sector information by reducing market entry barriers, in particular for small and medium-sized enterprises, by minimizing the risk of excessive first-mover advantage, which benefits large companies and thereby limits the number of users of the data in question, as well as by increasing business opportunities by encouraging the publication of dynamic data and the uptake of application programming interfaces (APIs).

2.5. Personal and non-personal data

30. The EDPS notes that the Strategy makes a distinction between **three categories of data**, namely non-personal, personal and mixed data sets. In this context, the EDPS would like to remind that in practice a combination of non-personal data may infer or generate personal data, i.e. data relating to an identified or identifiable individual.

31. The Strategy also refers to "**anonymised**" and "**aggregated**" data, at one point suggesting that the aggregated data might be the same than anonymized data.[22] Here the EDPS would like to point out that aggregated data is not necessarily non-personal data, since aggregated data might still be related to an identified or identifiable individual. In this regard, the EDPS recalls that, in line with Recital 26 of the GDPR and the case law of the CJEU[23], a due account should be taken of all objective factors, including the costs and the time required for identification, the available technology as well as the legal and other means to access additional data about the person.

32. Furthermore, anonymization processes are not straightforward[24]. The more varied the data, the more difficult it is to be anonymised by reducing the re-identification risk to an acceptable threshold. The practical difficulties associated with a robust anonymization process might prevent data controllers, and specially SMEs, from sharing valuable data. To reduce the required effort, while ensuring the data is anonymised appropriately, the EDPS encourages the Commission to

invest into and further support and foster good anonymization practices and anonymization standards.

33. In this regard, the EDPS would also like to point out to some best practices with reference to the re-use of anonymised data in the public sector, such as the extensive guidance developed by European Medicines Agency (EMA) for industry to facilitate compliance with this policy[25] or the provision of high quality as a 'public good' by the European Statistical System (ESS)[26].

2.6. European Union institutions, bodies and agencies

34. The EDPS notes that the Strategy does not specifically address the role and the applicable rules for the European Union institutions, bodies and agencies. It is true that data protection rules applicable to them, namely Regulation (EU) 2018/1725, is very much aligned with the GDPR and Directive (EU) 2016/680 and, consequently, all these acts have to be interpreted homogeneously[27]. At the same time, the Union institutions and other bodies are important actors in the data economy on their own - as providers of data (e.g. through EU Open Data Portal), users of data (e.g. for better policy making), or as service providers (e.g. the eHealth Digital Service Infrastructure[28]).

35. Hence, the EDPS, as the supervisory authority monitoring the personal data processing by Union institutions and bodies, is convinced that the Data Strategy and the related legal and non-legal acts on its implementation should take due account of the specific role of the European Union institutions, bodies and agencies. Thus the Union will not only ensure the necessary transparency and legal certainty but will also live up to Commission's promise in the Strategy to be "leading by example"[29].

3. DATA FOR SCIENTIFIC RESEARCH

36. The EDPS takes note of the Commission's plan to increase the amount and types of data available for scientific research in line with the principle 'as open as possible, as closed as necessary'. One of the key initiatives for facilitating discovery, sharing of, access to and reuse of data and services by researchers is the **European Open Science Cloud** (EOSC). The latter will also be used as a model for the creation of the future common European data spaces.

37. Both the EDPS Preliminary opinion on data protection and scientific research[30] and the EDPB Guidelines on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak[31] underline that **data protection rules, such as the GDPR, are fully compatible with and do not hinder genuine scientific research**. At the same time, sharing of personal data always involves a degree of risk to the data subjects, including where the purpose is scientific research, especially in cases of sensitive data. Data protection rules are intended to serve as a robust safety net for individuals whose data are needed to support science, as well as a framework steering researchers toward innovation that reflects the European values.

38. It is a common assumption that scientific research is beneficial to the whole of society and that scientific knowledge is a public good to be encouraged and supported. While the EDPS generally shares this viewpoint, performing an activity deemed to be research cannot be a *carte blanche* to take irresponsible risks on fundamental rights. From a data protection viewpoint, the principles of necessity, proportionality and purpose limitation are essential. As expressed in the Preliminary opinion on data protection and scientific research, data protection authorities, ethics committees and the research community have a common interest in working together to help the advancement of knowledge, while ensuring people are not treated as mere data sets.

39. While scientific research benefits from a special data protection regime, the EDPS would like to remind the Commission and researchers relying on the common data spaces that each of the principles under Article 5 of the GDPR (lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability) fully apply to any personal data processing for research purposes.

40. Scientific research often involves the processing and sharing of special categories of personal data of the people involved and thus, in certain cases, could be considered a high-risk data processing according to the GDPR. The EDPS therefore recommends that the **appropriate safeguards** are taken, and that access to the data stored in the data spaces is made on the basis of various factors, including but not limited to the actor requesting access; the purpose of the processing and its risk level; the existence of accountability frameworks and safeguards, etc. Furthermore, data protection impact assessments should be conducted when the research involves sensitive data, with the involvement the respective data protection officers (DPO) and ethical review boards.

41. The GDPR provides for derogations to certain obligations (i.e. providing the data subject's right of access (Article 15), right to rectification (Article 16), right to restriction (Article 18) and right to object (Article 21)) for scientific research purposes, where the processing is proportionate to the aim pursued, respects the essence of the right to data protection, and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Nevertheless, this special regime cannot be applied in such a way that the essence of the right to data protection is compromised. Derogations from these data subject rights must be subject to a particularly high level of scrutiny. They require a case-by-case analysis, balancing of interests and rights at stake, and a flexible multi-factor assessment. Any limitation to fundamental rights in law has to be interpreted restrictively and should not be abused. Furthermore, under Article 89(2) GDPR, derogations can be applied only "in so far as the rights to be derogated from are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes".

42. There is no universally agreed definition of research or scientific research. Moreover, boundaries between public interest, academic freedom and private gain today are more blurred than ever. This uncertainty may create loopholes in the protection of fundamental rights, including the right to privacy and to personal data protection. The EDPS therefore strongly recommends that the Strategy and the envisaged legislation address specifically the definitions and the scope of the key notions such as scientific research, innovation, public interest, to avoid inconsistency with existing notions in the GDPR[32].

4. COMMON EUROPEAN DATA SPACES

4.1. General comments on the concept

43. A key element of the Data Strategy is the development of common European data spaces in strategic economic sectors and domains of public interest. The data spaces would combine large pools of data, technical tools and infrastructures necessary to use and exchange data, as well as governance mechanisms. They would be governed by a horizontal framework complemented, where appropriate, by sectoral legislation for data access and use.

44. The common European data spaces fit into and support wider strategic objectives of the EU, such as the development of a fair and competitive **Digital Single Market**, uptake of new technologies like Artificial Intelligence and in particular machine learning, as well as asserting the **EU digital sovereignty**.

45. The EDPS welcomes the commitment in the Strategy that the common European data spaces will be developed "in **full compliance with data protection rules and according to the highest available cyber-security standards**" and looks forward to examining the specific proposals and initiatives aimed at implementing this commitment.

46. The EDPS welcomes the Commission's intention to consider the adoption of sector-specific legislation to accompany the creation of certain common European data spaces. The European legislator has a responsibility to put in place additional legal safeguards in situations where the Strategy would lead to increased availability and reuse of personal data. The need for further specification and particularisation of the general rules contained in the GDPR at EU level seems most pressing in relation to the sharing of health data and for scientific research in general. At the same time, such specification, aiming at the harmonization at the maximum possible extent of the rules on the processing of personal data for scientific research in particular, may further foster the sharing of data.

47. In addition to the horizontal data protection and cyber security standards, the Commission should invest in further fostering **interoperability**, including also in the context of data portability. Thus, the common data spaces would enable more data protection-compliant business models to emerge and thrive.

48. While the EDPS agrees that one-size-fits-all approach might not be appropriate, he nevertheless encourages the Commission to further clarify that the common European data spaces should be populated only with personal data which has been demonstrably obtained in compliance with data protection legislation, including in particular with the principles of lawfulness, purpose limitation and data minimisation.

49. According to the Strategy, data spaces will be used for multiple purposes. Hence, it should be clearly defined from the onset for each data space what are the permitted purposes (i.e. research and non-research, etc.). Moreover, the protection of the fundamental rights to privacy and to the protection of personal data, and the value of human dignity that underpins these rights, warrants, in certain scenarios, a clear limitation on the cross-context use of data, including **prohibitions on the use of sensitive personal data for other purposes** (for instance, the use of genetic data for insurance purpose). This is particularly relevant for the cross-sector use of personal data in the IoT context.

50. The common European data spaces, based on the European values and fundamental rights with the human being at the centre, could also serve as evidence of the **viability of alternative models** to the current concentration of data in the hands of a few private corporations based outside the EU which play the role of self-appointed gatekeepers of internet or big IT solution providers. Therefore, the envisaged European data spaces should serve as an example with regard to **transparency, effective accountability and proper balance** between the interests of the data subjects and the shared interest of the society as a whole.

51. The success of the common European data spaces and the Strategy as a whole depends heavily on the ability to create a solid level of **trust** between the various stakeholders - data subjects, governments, private companies, scientific research community and civil society organisations as well as data protection authorities and other relevant regulators. To this end, the governance model should specifically address the involvement of citizens and civil society.

4.2. Compulsory data sharing

52. The EDPS takes note of the Commission's intention to make **data sharing compulsory in certain circumstances**. There have been recent calls for regulated access across the EU to privately held personal data for research purposes that serve a public interest, such as improving healthcare provision and addressing the climate crisis[33]. Such initiatives are expected to become even more prominent in the context of COVID-19 pandemic. In addition, in his Preliminary opinion on scientific research, the EDPS has highlighted the issue of corporate secrecy, particularly in the tech sector, which controls some of the most valuable data, as a major barrier to social science research.

53. A possible public interest basis under data protection law to disclose data has to be clearly formulated and laid down in EU or Member State law, as well as to be accompanied by a rigorous proportionality test and appropriate safeguards against misuse and unlawful access. Therefore, the EDPS recommends an **open and inclusive debate** on this matter, which should involve all stakeholders, such as the research community, tech companies, civil liberties groups, supervisory authorities, etc.

54. Finally, the EDPS calls for cautious approach towards initiatives aimed at compulsory **access to personal data in the competition context**, i.e. access to personal data held by the incumbent undertaking by its competitors. Such sharing and access to data among competitors must be balanced against other policy concerns, especially data protection. Any sharing or access to personal data must be strictly defined in scope and purpose and must occur in full compliance with the GDPR, taking into account the requirements of lawfulness, purpose limitation and the legitimate expectations of users.

4.3. Common European Health Data Space

55. One of the nine strategic sectors, where the Commission sees a clear added value for the Union from pooling of data and technical resources, is **healthcare**. The objective of the proposed common European health data space is to improve access to and quality of healthcare, support scientific research and help competent authorities in taking evidence-based policy decisions.

56. Given the significant impact and sensitiveness of cross-border exchange of health data, the EDPS wishes to highlight that all processing operations, which might result from the establishment of a common European health data space, will require a **robust legal basis** in line with EU rules on data protection. In this regard, he also points out to the need for **further harmonization of data protection rules applicable to health data** among the Member States. In addition, a European Code of Conduct on the processing of health data for the purpose of scientific research could be an effective enabler for greater cross-border exchange of health data within the EU.

57. Sharing of health data could play an important role in addressing important individual and societal problems, when accompanied by appropriate data protection safeguards. The outbreak of COVID-19, which has affected our lives in an unprecedented way, has very convincingly underlined that. In this regard, the EDPS recognises that data sharing could substantially contribute in managing the current crisis and its long-term consequences, as well as help the EU prepare for possible future crises of a similar nature.

58. The EDPS would like to draw the attention on 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 which highlight and further explain the essential data protection requirements, in particular legality, transparency, necessity and proportionality, as well as

integrity and confidentiality. Personal data may only be processed for specified legitimate purposes, where necessary for these purposes, and not used in a way incompatible with those purposes.

59. Finally, while acknowledging the limits of Union competence in the area of healthcare, in accordance with the Treaties, the EDPS invites the Commission to consider the possible role of the envisaged European health data space as an instrument for **better preparedness, reaction and management of future health-related crises**, together with the eHealth Digital Service Infrastructure (eHDSI) and others relevant EU structures and initiatives.

5. SPECIFIC ISSUES

5.1. Governance frameworks for data access and use

60. The EDPS shares the view of the Commission that putting in place an enabling **legislative governance framework** is a priority for operationalising the Data Strategy and its core element - the common European data spaces. It should ensure legal certainty and consistency with other existing legal frameworks, in particular on data protection, by building upon and reinforcing them.

61. The EDPS expects to be consulted on the future legislative proposals, such as the envisaged Data Act, in accordance with Article 42 of Regulation 2018/1725. Without prejudice to his future opinion(s), the present Opinion on the data strategy aims to provide some preliminary comments and recommendations related to the governance framework.

62. Depending on the risks, nature, scope, context and purposes of processing, some type of formal **"vetting"** of organisations requesting access to common European data spaces might be warranted, for example in the form of a Clearinghouse. Furthermore, organisations involved in data pooling or sharing arrangements should adhere to certain common standards, not just in terms of interoperability, but also with a view of ensuring lawfulness of processing and facilitating data subject rights (e.g. through joint controller arrangements pursuant to Article 26 of the GDPR).

63. Next, to ensure data controller accountability, the governance framework should include **data traceability** requirements. This is particularly relevant for the common European data spaces which would combine data from different Member States and from various sources, both public and private.

64. Finally, the EDPS underlines that in the context of future governance mechanisms the competences of the **independent supervisory authorities for data protection** must be properly respected. Moreover, the implementation of the Strategy leading to wider use of data will require a significant increase of resources for DPAs and other public oversight bodies, in particular in terms of technical expertise and capabilities. Cooperation and joint investigations between all relevant public oversight bodies, including data protection supervisory authorities, should be encouraged.

5.2. Privacy preserving technologies

65. The EDPS appreciates the fact that the Strategy identifies privacy preserving technologies as "crucial for the next stages of the data economy". In the same spirit, the EDPS recalls the potential of **privacy enhancing technologies** (PETs) as enablers of data sharing which is both privacy-friendly and socially beneficial.

66. There are a number of promising technological solutions, such as use of **synthetic data**, which may, *inter alia*, facilitate access to training data for machine learning. While there are still uncertainty and open questions related to possible feasibility and the efficacy of such solutions to mitigate data protection risks, the EDPS encourages the Commission to invest in further research and tests.

67. In addition, in order to optimise the benefits of the various privacy preserving technologies, the EDPS emphasizes the importance of their **standardization and interoperability**. To this end, he welcomes the commitment in the Strategy for facilitation of the development of common European standards and requirements for the public procurement of data processing services and encourages the Commission to pursue further this objective.

5.3. 'Data altruism'

68. In the Strategy the Commission commits to "make it easier for individuals to allow the use of the data they generate for the public good, if they wish to do so ('data altruism'), in compliance with the GDPR". In relation to the concept of "data altruism", also described as "data donation", the EDPS considers that the added value of this notion is not entirely clear, taking into account that such 'data altruism' would rely on the consent of the data subject and that the GDPR already provides principles and rules on consent. Therefore, the EDPS invites the Commission to better define and lay down the scope, including the possible purposes, of such "data altruism" (for instance, data altruism for scientific research in the health sector).

69. The EDPS would also like to reiterate that the fundamental right to the protection of personal data cannot in any case be 'waived' by the individual concerned, be it through a "donation" or through a "sale" of personal data. The data controller remains fully bound by the personal data rules and principles even when processing data that have been "donated" i.e. when consent to the processing had been given by the data subject.

5.4. Skills and digital literacy

70. The EDPS welcomes the commitment of the Commission to **invest in skills and general data literacy**. In this regards, he would like to stress that data protection literacy is important for individuals to know their rights in general and to make informed decisions about whether or not to allow certain uses of their data. This is particularly relevant for young people who are among the most active users of digital services.

71. Data protection awareness is a *conditio sine qua non* for ensuring that individuals' consent is meaningful. Furthermore, data protection conscious individuals would make better use of their data subject rights and thus would push all actors in the data ecosystem to comply with the letter and the spirit of the GDPR.

5.5. International data sharing

72. The EDPS welcomes the clear commitment that all companies and other organisations which sell goods or provide services related to the data economy in Europe must respect European legislation and this should not be compromised by jurisdictional claims from outside Europe.

73. The EDPS would like to recall that all **transfers of personal data to third countries or international organisations** must comply with Chapter V and the other relevant provisions of the GDPR, or in the case of Union institutions and bodies, with Regulation (EU) 2018/1725. This obligation fully applies to **cloud computing**, as illustrated by the EDPS Guidelines on the use of

cloud computing services by the EU institutions and bodies[34] and the establishment of the Hague Forum - the first EU software and cloud suppliers customer council[35].

74. The EDPS fully shares the view of the Commission that international cooperation must be based on an approach that promotes the EU's fundamental values, including protection of privacy and personal data. The same approach is guiding the EDPS in his cooperation with other partner organisations and within international fora such as the Global Privacy Assembly.

6. CONCLUSIONS

75. The EDPS understands the growing importance of data for the economy and society and supports the ambition to make the European Union "the most attractive, most secure and most dynamic data-agile economy in the world". At the same time, he would like to recall that "big data comes with big responsibility" and therefore appropriate data protection safeguards must be in place and effectively applied.

76. The EDPS welcomes the Commission's commitment to ensure that European fundamental rights and values, including the right to the protection of personal data, underpin all aspects of the Data Strategy and its implementation. In particular, he appreciates the assurance that the Strategy would be developed in full compliance with the General Data Protection Regulation, which provides a solid basis, also by virtue of its technologically-neutral approach.

77. Today, the predominant business model of the digital economy is characterised by unprecedented concentration of data in the hands of a handful of powerful players, based outside the EU, and wide-scale pervasive tracking. The EDPS strongly believes that one of the most important objectives of the Data Strategy should be to prove the viability and sustainability of **an alternative data economy model** - open, fair and democratic. Therefore, the envisaged common European data spaces should serve as an example of transparency, effective accountability and proper balance between the interests of the data subjects and the shared interest of the society as a whole.

78. The EDPS expects to be consulted on any legislative follow-up to the Data Strategy which will have an impact on data protection, as set out above, in line with Article 42 of Regulation 2018/1725, and remains at the disposal of the Commission, the Council and the European Parliament to provide further advice at the next stages of implementation of the European strategy for data, both in terms of legal framework and of practical aspects. The comments in this Opinion are without prejudice to additional comments in the future on particular issues and/or if further information is available.

Brussels, 16 June 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/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy
[5] COM(2020) 67 final, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en
[6]COM(2020) 65 final, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_en
[7] https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf
[8] https://edps.europa.eu/sites/edp/files/publication/18-07-11_psi_directive_opinion_en.pdf
[9] https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf
[10] See more at https://edps.europa.eu/data-protection/our-work/subjects/covid-19_en
[11]COM (2017) 10 final, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)
[12] See Article 29 Working Party Guidelines on Transparency under Regulation 2016/679 (wp260rev.01) https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025
[13] https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf
[14] https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem
[15] See Recital 4 of GDPR
[16] See Article 29 WP Guidelines on DPIA: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
[17] In this regard, the general rule under Article 12(1) of the Open Data Directive states, subject to the limited exception under Article 12(2): "The re-use of documents shall be open to all potential actors in the market, even if one or more market actors already exploit added-value products based on those documents. Contracts or other arrangements between the public sector bodies or public undertakings holding the documents and third parties shall not grant exclusive rights."
[18] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, OJ L 345, 31.12.2003, p. 90.
[19] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.6.2019, p. 56-83.
20 EDPS Opinion 5/2018, Opinion on the proposal for a recast of the Public Sector Information (PSI) re-use Directive, available at: https://edps.europa.eu/sites/edp/files/publication/18-07-11_psi_directive_opinion_en.pdf
[21] See, for instance, the Data protection impact assessment for smart grid and smart metering environment, available at:https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force/data-protection-impact-assessment-smart-grid-and-smart-metering-environment The latter could be implemented in order to also take into account the re-use of data to identify energy saving solutions.
[22] See at page 8 of the Strategy, referring to "use of aggregated and anonymised social media data".
[23] See Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779
[24] See Article 29 WP Opinion 05/2014 on Anonymisation Techniques, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
[25]https://www.ema.europa.eu/en/human-regulatory/marketing-authorisation/clinical-data-publication/support-industry-clinical-data-publication
[26] https://ec.europa.eu/eurostat/web/european-statistical-system/reuse-ess-statistics
[27] See Recital 5 of Regulation (EU) 2018/1725
[28] See 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://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12019-processing_en
[29] See page 15 of the Data Strategy.
[30] https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf
[31] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en
[32] See more on this issue in the EDPS Preliminary opinion on data protection and scientific research
[33] See for instance the opinion of the German Data Ethics Commission from 2019, recommendations 16-23.
[34] https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf
[35] For more information see https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigation-it-contracts-stronger_en