JOAL Special issue on "Open Science and Data Protection"
Part II Commentary:

The protection of personal data for the purpose of scientific research and the Open Science framework: Ongoing challenges and future opportunities.

Veronique Ciminà[a]
[a] *European Data Protection Supervisor (EDPS)**

Abstract. The following contribution aims to provide concluding remarks on the special issue on "Open Science and Data Protection". Following some general introductory considerations, the paper will first focus on scientific research and the GDPR: within that framework, it will address (i) the legal basis for the processing of personal data for scientific research purposes and in particular (ii) consent as a legal basis in research. The contribution continues by addressing the use of Open Data for the public benefit and secondary use of health data more generally. It concludes by looking at the future, in particular at European initiatives, such as the forthcoming European Health Data Space (EHDS) and its objective to enhance data sharing, ensure compliance with the data protection regulatory framework and safeguard the freedoms and rights of individuals.

Keywords: Data protection, scientific research, consent, Open Science, anonymisation, privacy-enhancing technologies, European Health Data Space

1. Introductory remarks

Scientific research is fundamental for the exchange of information and "for the construction of a public deliberation" (Paseri, 2021, 159), thus contributing to the advancement of generalisable knowledge, which has become a key priority for the EU in the last years. Where scientific research processes personal data of people in the EU, it is subject to the rules set out in the General Data Protection Regulation (GDPR)[1]

* The views expressed by the author in this article are personal and do not represent the views of the European Data Protection Supervisor (EDPS).

[1] 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), ELI: http://data.europa.eu/eli/reg/2016/679/oj.

and Regulation (EU) 2018/1725 (EUDPR)[2]. Such rules offer a special flexibility regime for genuine research projects operating within an ethical framework and aiming at increasing societal and collective wellbeing and knowledge. The practical functioning of the scientific research data protection regime has been discussed at length and work is also ongoing on the side of the European Data Protection Board (EDPB) to interpret specific provisions of the GDPR in this regard. While some argue that the GDPR does not offer enough flexibility to operate scientific research, others, as also explained by Giorgia Bincoletto in the paper 'Scientific research processing health data in the European Union: Data Protection regime vs Open Data' contained in this issue, are of the view that such framework "does not hamper but rather encourages data-driven framework" (Bincoletto, 2023, 9).

Moreover, digitalisation has brought to the transformation of research and to a wider availability of data, the sharing of which is encouraged at EU level for research purposes. Therefore, EU initiatives and legislative measures enacted throughout the years have aimed at making data available for re-use, in order to foster innovation and research. Such initiatives range between the Open Access Infrastructure for Research in Europe (OpenAIRE) project and the European Open Science Cloud (EOSC), Regulation (EU) 2021/695 establishing Horizon Europe - the Framework Programme for Research and Innovation and Directive (EU) 2019/1024 on Open Data and the re-use of public sector information.

However, despite such initiatives, "[a]n analysis of the current legislation seems to indicate several legal constraints on the circulation of data (information, knowledge, and material), able to affect the building of an effective European Data Area" (Colcelli and Cippitani, 2023, 1).

Against this background, the papers contained in this issue perfectly identify the main challenges and concerns to be addressed by legislation in order to foster a functioning European Data Area with effective data protection safeguards. The sections below highlight the main ongoing challenges, with the goal of identifying possible interpretations and solutions.

[2] 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj.

2. Scientific research and the GDPR

The GDPR offers a special regime for the processing of personal data for scientific research purposes. While each principle under Article 5 of the GDPR applies to all data processing, including research, it also contains several provisions which give EU Member States the authority to implement and adapt the GDPR at national level, including the adoption of provisions covering the processing of health data for scientific research purposes. Article 89 of the GDPR, in this sense, provides for flexibility in the obligations on controllers and puts an emphasis on adequate safeguards and accountability. Additionally, Article 9(2)(g) to 9(2)(j) of the GDPR permit derogations to the prohibition of the processing of special categories of personal data on the basis of EU or Member State law, including for the purposes of scientific research. Lastly, under Article 9(4) of the GDPR, Member States may also enact "(...) further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health".

However, despite such special regime afforded by the GDPR to scientific research, the interpretation of such provisions and, specifically, their application in the context of cross-border activities within the EU, remains uncertain. Indeed, as highlighted by Valentina Colcelli and Roberto Cippitani in their paper 'Circulation of personal data and non-personal data within the European Research Area for research and health purposes', "[t]he GDPR enables data flows for research cooperation in the EU, but the rules at the national level regarding research exemptions create a hurdle for cross-border research by ignoring the intra-EU conflict of laws that inevitably arise in a fragmented regulatory framework." Such lack of harmonisation is particularly exemplified by the diverse additional national laws and rules related to health and research data, the different legal bases chosen by Member States for the processing of personal data for scientific research purposes and their ability to set their own derogations under the GDPR.

European Data Protection Authorities have acknowledged such issues by having made multiple attempts to clarify the GDPR provisions relating to scientific research, including, but not limited to, the presumption of compatibility under Article 5(1)(b) GDPR, the notion of 'broad consent' (Recital 33 GDPR), information to be provided to data subjects and the safeguards under Article 89(1) GDPR. In this regard, the EDPB has also clarified that "[i]t is important that this regime is not perceived as to imply a general exemption to all requirements in the GDPR in case of processing data for scientific research purposes. It should be taken into account that this regime only aims to provide for exceptions to specific requirements in specific situations and that the

use of such exceptions is made dependent on 'additional safeguards' (Article 89(1) GDPR) to be in place" (EDPB, 2021, p. 4).

Moreover, the EDPB is currently working on specific guidelines, which will elaborate further on the elements highlighted above while also aiming to provide a more comprehensive interpretation of the various provisions in the GDPR, relevant for the processing of personal data for scientific research purposes.

3. Legal basis for the processing of personal data for scientific research purposes

One of the main elements burdening cross-border research often lays in the different legal basis chosen by Member States for the processing of personal data for scientific research purposes. In its response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research, the EPDB highlighted that "(...) it can be observed that in Member State laws considerable differences can be found in legal bases for processing health data for scientific research purposes are either specified, prescribed or excluded and whether an exemption on Article 9(1) based on Article 9(2)(g), (i) or (j) GDPR has been foreseen (with additional requirements) in Member State law" (EDPB, 2021, p. 5).

In this regard, the EDPB, understanding the practical consequences that the use of different legal bases for processing of personal data may have on cross-border research, has provided guidance on how to attempt approaching such issue. In particular, in its 'document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research', the EDPB recommends to use, when conducting research projects in multiple Member States, the same legal basis in the project, whenever possible. On the other hand, the EDPB also acknowledges the likely foreseeability of a heterogeneous legal basis for the processing of personal data of the participants in a single research project carried out in several Member States, due to national legislation put in place at Member State level. However, as rightly pointed out in the same document, it also confirms that such lack of homogeneity between legal bases may not be solved by the EDPB alone or by means of Codes of Conduct within the meaning of the GDPR.

To this end, among the legal bases listed under the GDPR, consent deserves a special mention. First, it is worth underlining that consent within the meaning of the GDPR should be distinguished from the ethical standard requiring the collection of informed consent as human

participant in a research study and/or protocol. In this regard, the EDPB highlights that controllers should pay specific attention to the condition of 'freely given' consent within the meaning of the GDPR and that consent should not be the chosen legal basis for the processing of personal data where a clear imbalance exists between the controller and the data subject (EDPB, 2019, par. 18). In the same Opinion, the EDPB clarifies that, although informed consent may be adequate, a clear situation of imbalance of powers between the participant and the controller will imply that consent is not 'freely given' within the meaning of the GDPR. Therefore, as concluded by the EDPB, consent may not always be the most appropriate legal basis in most cases, and other lawful grounds of processing provided under Article 6(1)(e) or 6(1)(f) GDPR may be more appropriate.

In this respect, the empirical data collection and analysis process, presented by Dara Hallinan, Franziska Boehm, Annika Külpmann and Malte Elson in their paper "(Un)informed consent in Psychological Research: empirical study on consent in psychological research and the GDPR" aimed at understanding to what degree the consent processes in psychological research in Europe fulfill the GDPR requirements laying down the forms of information to be provided to research subjects, perfectly highlights the practical challenges in ensuring GDPR compliance in the research sector. As the study concludes, "[t]he results did not paint the evaluated consent procedures in a positive light" (Hallinan, *et al.*, 2023, 24), thus proving a significant misalignment between the information provided in consent materials and the information provision requirements under the GDPR. In particular, such results identify three specific issues, namely 1) the provision of inadequate information, both in the form of the provision of false or misleading information and of a lack of provision of adequate information; 2) terminological misalignment, where GDPR terminology is presented in a contradictory and confusing way; and 3) the actual structure of consent materials, very often presented in a lengthy and complex way. The authors of the study also find that the above-mentioned issues are predominantly a result of the lack of familiarity of researchers with European data protection law and that guidance in that sense would be needed.

The study seems to support that an overlap exists between informed consent of participants in a research project and consent as a legal basis within the meaning of the GDPR. However, viewing "(...) them as a single and indivisible requirement would be simplistic and misleading" (EDPS, 2020, p. 19). Indeed, given the specific requirements that consent as a legal basis under the GDPR needs to fulfil, this may not be the most suitable legal basis for data processing and other lawful grounds under both Articles 6 and 9 GDPR should be considered. However,

informed consent as a participant in a study could still be used as an 'appropriate safeguard' of the rights of data subjects.

To this end, it is fundamental that Data Protection Authorities (DPAs) support researchers and data subjects in applying the most appropriate legal grounds and safeguards in order to foster a better legal understanding and effectiveness of the studies and processing activities carried out within the any single Member State and across the EU. Moreover, legislative initiatives such as the forthcoming European Health Data Space (EHDS) Proposal[3] may offer concrete possibilities for cross-border use of (electronic) health data to take place, as will be argued below.

4. Use of Open Research Data for the public benefit

In the last years, more than ever before, global crisis such as the COVID-19 pandemic, have accelerated the need to share data with the aim of providing services for the public benefit. Despite such need, public authorities are often unable to address and confront such emergencies. However, as argued by Anna Berti Suman in the paper 'Citizen-gathered data to support public services under emergencies: promises and perils of openness', "[i]n light of the perils of openly sharing citizen-gathered data to address emergencies, for example with researchers and institutions, regulating such practices seems advisable. In other words, such decentralized and informal data flows which at the moment do not follow specific regimes for data sharing and storing may need to fit existing legal provisions, or new legal instruments may need to be formulated to regulate them" (Berti Suman, 2023, p. 2).

In this regard, the paper clearly explains that literature is not aligned on the notion of 'public benefit', with diversified terminology being used, including public interest, public good, public benefit etc., thus creating social and legal uncertainty. In this regard, legislative initiatives such as the Data Governance Act (DGA)[4] and the EHDS aim at fostering and setting out the modalities for the sharing of data (and health data in the context of the EHDS Proposal) for the public benefit. The DGA *de facto* introduces the concept of 'data altruism', defined as the "(...) voluntary sharing of data on the basis of the consent of data

[3] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM/2022/197 final, ELI: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0197.

[4] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), ELI: http://data.europa.eu/eli/reg/2022/868/oj.

subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest" . On the other hand, the EHDS Proposal, foresees the establishment of additional criteria, given the sensitivity of the data to be processed.

As rightly pointed out in the paper, "[p]ublic benefit is often understood way beyond an individual level, encompassing indirect benefits such as enhanced knowledge on a certain matter for a (more or less broadly understood) community" (Berti Suman, 2023, 9). However, global crisis such as the COVID-19 pandemic have accelerated the discussion on the practical evidence required to define 'public benefit' as such, often outweighing concerns for data protection and privacy risks for the personal data shared. Indeed, "greater reliance on decentralised citizen-gathered data flows coming from spontaneous civic initiatives to innovate interventions in crisis scenarios" (Berti Suman, 2023, 20) may be an opportunity. To that end, the studies reflected in the same paper underline that such methods and approaches could provide for practical and sound guidance on how to rely on such flows both scientifically and legally. Based on the observations made above, some preliminary considerations can be made concerning the use of data for the public benefit.

First, it is crucial to pay renewed attention to the notion of 'public benefit'. Indeed, providing a precise definition of such notion would not only ensure legal certainty, for example when interpreting provisions such as data altruism, but would also assure that data sharing activities are not misused for gains other than societal ones. Therefore, in the light of ensuring data sharing while at the same time protecting the fundamental right to data protection and privacy of citizens, it is essential to interpret such notion in a more circumscribed manner.

Second, a more coordinated and effective use of data for public benefit purposes is required. In order for data protection to continue fulfilling its role in enhancing trust when using and sharing data in emergency situations for the public benefit, the data protection community and DPAs will need a more active engagement with experts from the public health community, international organisations, researchers and civil society.

Third, while acknowledging that "the burst in crises (some of which unexpected) of the last decade, posing wicked problems to institutions, researchers and society at large, cannot be addressed only through top-down, tech-driven and centralized interventions" (Berti Suman, 2023, 21), legislation should bridge the gaps by providing clear definitions of concepts such as 'public benefit' and by identifying the criteria, modalities, infrastructures and safeguards for the sharing of data for such use. Only in such way societies and democracies can increase public trust and legitimise legislative and institutional interventions, while at the same time ensure that public benefit does not collide with data protection and privacy rights of citizens.

5. Secondary use of health data: enhancing data sharing while fostering compliance

In the context of the debate and legislative developments on Open Science, the exchange of data in the biomedical field occupies a privileged position. As mentioned above, global crisis such as the COVID-19 pandemic have brought consensus on the need to share health and biomedical data while at the same time introducing technical and legislative safeguards to enhance trust of patients and citizens. From a legislative perspective, the European Commission's EHDS Proposal aims at achieving such objective, with "(...) the potential to overcome some of the legal issues around technical solutions available" (Abu Attieh, *et al.*, 2023, p. 8)

In addition to setting out rules for the processing of electronic health data for primary use, the EHDS Proposal aims at facilitating the secondary use of electronic health data for purposes such as research, innovation, policy making, patient safety or regulatory activities. Moreover, it defines a set of data types to be used and processed for defined purposes, as well as prohibited purposes, and contains provisions relating to the governance of such secondary use and the consequent establishment and functioning of health data access bodies, responsible, among others, for the issuance of permits to data applicants accessing data made available by data holders. Therefore, as outlined by Hammam Abu Attieh, Anna Haber, Felix Nikolaus Wirth, Benedikt Buchner and Fabian Prasser in their paper 'Enabling Open Science in Medicine Through Data Sharing: An Overview and Assessment of Common Approaches from the European Perspective', the Proposal shows "a clear intention to foster the utilization of data for research purposes. At the same time, improvements in privacy-enhancing technologies provide increasingly more favourable trade-offs between privacy risks and the

usefulness of data sharing platforms. These are good signs for a broader adoption of Open Science principles in medicine" (Abu Attieh, *et al.*, 2023, 8).

Indeed, scientists are utilising new technologies to bring greater assurances of research participant autonomy and privacy in 'privacy enhancing technologies' (PETs), which are referred to "privacy-preserving data sharing and analytics technologies that enable data sharing and analysis among participating parties while maintaining dissociability and confidentiality" (Kurapati and Gilli, 2023, 6). The security strategies covered in the paper – which include both cryptographic and distributed approaches, as well as safe havens and legislated protections – might serve as a standard more broadly for how personal data, including behavioural and biological data, are treated to allow the social and commercial value of aggregated data to be realised without putting individuals at risk. The categorisation of security measures outlined in the paper also suggests that we may have reached a point where respecting the autonomy of research participants could entail informing them of the data security methods that the study is deploying. In order to expand the scope of Open Science, it appears that the improved data security strategies that Abu Attieth *et al.* identify, create greater opportunities for research participants to exercise their informed autonomy. In fact, increased participant rights do not need to diminish the role of scientific expertise in directing the research. On the other hand, it can ensure that science keeps up with the increased societal concerns related to surveillance capitalism (Zuboff, 2019) by advancing the democratic force of individual autonomy. Through the exercise of such autonomy, participants would be, to a greater degree than previously, acting on the world.

Against this background, it is essential to understand to what extent PETs, such as multiparty computation, homomorphic encryption, federated learning, secure enclaves, differential privacy and synthetic data generation, may foster responsible innovation while at the same time ensure compliance with data protection legislation. Shalini Kurapati and Luca Gilli in their paper "Synthetic data: A convergence between Innovation and GDPR" aim to explain the opportunities and challenges presented by synthetic data for GDPR, particularly with regard to scientific research. As highlighted in the paper, "[t]he common opinion among data practitioners, and professionals applying innovation in organizations on GDPR is that it only restricts data processing, thereby stifling innovation. While the private sector has commercial and business strategy constraints on top of legal compliance issues, accessing and sharing personal data is complex even in research settings where the awareness and resources for doing it efficiently are lacking" (Kurapati

and Gilli, 2023, 2). Moreover, the scenario is even more complex when a research project involves public-private collaboration, as shown by Anat Lior in the field of Artificial Intelligence research (Lior, 2023).

Despite this being the general opinion, new technologies such as the ones presented in the paper seem to bridge the gap between the need to foster innovation while at the same time preserving data protection and privacy of individuals. In fact, techniques such as anonymisation "(...) do not necessarily produce anonymous data, according to the GDPR" and "[t]he risk of re-identification of an individual from that data is zero" (Kurapati and Gilli, 2023, 5). As also confirmed by the EDPB, "[i]t should be taken into account that anonymisation of personal data can be difficult to achieve (and upheld) due also to ongoing advancements in available technological means, and progress made in the field of re-identification. For this reason, the anonymisation of personal data should be approached with caution in the context of scientific research" (EDPB, 2021, p. 11). Moreover, full anonymisation is often argued to compromise the effective results of studies.

To this end, among PETs, special attention is currently being paid to the use of synthetic data, which can be "thought of as artificial data that closely mimic the properties and relationships of real data". Indeed, "[u]sing synthetic data may represent a safe proxy for real data since it contains no real personal information for several AI and analytics use cases, such as data science/AI projects, test automation, and, most importantly, privacy preservation" (Kurapati and Gilli, 2023, 6).

Moreover, as outlined in the paper by Shalini Kurapati and Luca Gilli, key advantages of synthetic data include effective protection mechanisms against direct re-identification, compliance with data protection by design and the capturing of statistical characteristics of high-dimensional datasets by providing a more precise portray of complex datasets while at the same time safeguarding individuals' privacy. However, possible shortcomings of synthetic data in relation to personal data protection relate to the lack of application maturity and identifiability of specific synthetic data generation methods.

Considering the rapid development of synthetic data, studies are being carried out on the topic[5], some also including specific recommendations to data developers, researchers, regulators and policymakers with respect to its use and deployment, particularly in relation to data protection and privacy of individuals. However, more generally, the paper indicates that "[a]lthough supervisory authorities and regulators are closely following the application of PETs, such as synthetic

[5] See, for instance, Mitchell and Redrup Hill, 2023, 66, A PHG Foundation report independently commissioned by the MHRA to assess the status of synthetic health data in UK data protection law.

data, still a gap in legal certainty persists. In other words, there is no assurance to companies that such technologies are GDPR compliant, even though they are more effective than "approved" methods such as anonymization" (Kurapati and Gilli, 2023, 9).

To this end, the EHDS Proposal will be fundamental to allow secondary use of data for a variety of purposes, including healthcare delivery, research, innovation and policy making, while at the same time providing for a robust legal basis for processing in line with EU data protection law, the establishment of a strong data governance mechanism and effective safeguards for the rights of natural persons, in full compliance with the GDPR. On the other hand, as highlighted by the EDPS and the EDPB in their Joint Opinion on the EHDS Proposal, a lack of proper delineation of purposes for which data may be processed for secondary use may pose tangible risks for individuals' data protection rights (EDPS-EDPB, 2022).

6. Concluding remarks

The papers contained in this special issue have identified and outlined the main ongoing challenges and future opportunities concerning scientific research under the GDPR and the Open Science framework, starting from the contributions of the JOAL Special Issue on "Open Science and Data Protection". Such challenges range from the interpretation of the GDPR provisions on scientific research, to the legal bases for the processing of personal data for scientific research purposes, to the Open Science framework and the processing of data for public benefit and for other purposes, including innovation.

It is clear that, in the light of the discussions, tension exists between the data protection legal framework, Open Data policies and what Ludovica Paseri defined as the "research data paradox of the contemporary science" between "the pursuit of data-driven scientific research on the one hand and, on the other, the overwhelming challenges of repeatability of such data-driven research projects and their results" (Paseri, 2023, 2). While the sharing of data for purposes such as research, innovation, policy-making, and regulatory activities is fundamental, at the same time, the use of personal health data requires full compliance with the data protection framework in order to safeguard the fundamental rights and freedoms of individuals.

However, despite such tension, it would be inaccurate and simplistic to conclude that the data protection legal framework and Open Science are in contrast with one another. Indeed, the papers contained in this issue are proof that multiple attempts are being made to ensure data

sharing while complying with data protection rules, not only from a legislative perspective, but also from a technical and organisational one. Moreover, it is also evident how the legislative initiatives currently being adopted and/or proposed such as the DGA and the EHDS, confirm that, in order to achieve the fundamental objective of sharing of data for the public benefit, a solid legal context must be built. This should not only be reflected in the actual legal sources but especially in a robust legal basis for processing, in the establishment of a strong data governance mechanism and effective safeguards for the rights and interests of data subjects, in full compliance with data protection law.

It is too early to determine whether legislative initiatives such as the forthcoming EHDS will be enough to ease the tension between the data protection legal framework and Open Science. However, it is crucial to address the most problematic issues at hand such as, among others, the interplay between the types of secondary use with the grounds for exception foreseen in Article 9(2) GDPR, the legal basis for cross-border exchange of data for secondary use, and the exercise of data subject's rights. Starting by addressing such issues is the most effective way to achieve a balance which takes into account the objectives pursued and the protection of personal data of the data subjects affected by the processing.

Acknowledgements

Special thanks to Prof. John Willinsky, for his valuable insights and for his cooperation, especially in providing input on one of the papers of this JOAL special issue.

References

Abu Attieh, H., Haber, A., Wirth, F. N., Buchner, B., Prasser F., (2023), *Enabling Open Science in Medicine Through Data Sharing: An Overview and Assessment of Common Approaches from the European Perspective*, in Paseri, L., "Special issue on Open Science and Data Protection", Journal of Open Access to Law, 2023, vol. 11, no. 2, pp. 1-10.

Berti Suman, A. (2023), *Citizen-gathered data to support public services under emergencies: promises and perils of openness*, in Paseri, L., "Special issue on Open Science and Data Protection", Journal of Open Access to Law, 2023, vol. 11, no. 2, pp. 1-24.

Bincoletto, G. (2023), *Scientific research processing health data in the European Union: data protection regime vs. open data*, in Paseri, L., "Special issue on Open Science and Data Protection", Journal of Open Access to Law, 2023, vol. 11, no. 2, pp. 1-24.

Colcelli, V., Cippitani, R. (2023), *Circulation of personal data and non-personal data within the European Research Area for research and health purposes*, in Paseri, L., "Special issue on Open Science and Data Protection", Journal of Open Access to Law, 2023, vol. 11, no. 2, pp. 1-24.

EDPB (2021) *EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/edpb-document-response-request-european-commission_en.

EDPB (2019) *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b))*, https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_en.

EDPB-EDPS (2022) *Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space*, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en.

EDPS (2020) *A Preliminary Opinion on data protection and scientific research*, https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

Hallinan, D., Boehm, F., Külpmann, A., Elson, M. (2023), *(Un)informed consent in Psychological Research: An empirical study on consent in psychological research and the GDPR*, in Paseri, L., "Special issue on Open Science and Data Protection", Journal of Open Access to Law, 2023, vol. 11, no. 2, pp. 1-28.

Kurapati, S., Gilli, L. (2023), *Synthetic data: A convergence between Innovation and GDPR*, in Paseri, L., "Special issue on Open Science and Data Protection", Journal of Open Access to Law, 2023, vol. 11, no. 2, pp. 1-12.

Lior, A., (2023), *Private and Academic AI Collaboration: Opportunities and Challenges to Open Science in the US*, in Paseri, L., "Special issue on Open Science and Data Protection", Journal of Open Access to Law, 2023, vol. 11, no. 2, pp. 1-14.

Mitchell C., Redrup Hill E. (2023),*Are synthetic health data 'personal data'?* , PHG Foundation report.

Paseri L. (2023), *Open Science and Data Protection: Engaging Scientific and Legal Contexts*, in Paseri, L., "Special issue on Open Science and Data Protection", Journal of Open Access to Law, 2023, vol. 11, no. 2, pp. 1-28.

Paseri, L. (2021), *COVID-19 Pandemic and GDPR: When Scientific Research becomes a Component of Public Deliberation*, in Hallinan, D., Leenes, R., and De Hert, P. (Eds.), "Data Protection and Privacy: Enforcing Rights in a Changing World", Hart Publishing, Oxford, pp. 157-185.

Zuboff S., (2019) *Surveillance Capitalism and the Challenge of Collective Action*, New Labor Forum, 28(1), pp. 10–29.