Editorial

Data protection and research: A vital challenge in the era of COVID-19 pandemic

The issue of data protection in research is becoming of pivotal importance, in particular in the last months with the pandemic emergency of COVID-19. Studying the development of the outbreak on affected populations under a scientific and statistic perspective is necessary to understand the trend of contagion, the effectiveness of social distancing measures, the most vulnerable people who are the target of the virus, etc. This has posed several questions in terms of privacy and data protection. Medical researchers and even data scientists might use health data of patients for secondary purposes, different from the original purpose of the mere provision of healthcare services. In addition, researchers might analyse telcom data, such as location data, of patients (or just of citizens of mostly affected area) to understand their movements and the spread of the virus. Also, beyond research, these data have high potentials for further purposes (state surveillance on infected people, the enforcement of social distancing rules, etc.), and related high risks for fundamental rights and freedoms of data subjects (discrimination, stigmatization, unnecessary state surveillance and related chilling effect, profiling for manipulative purposes, etc.).

Accordingly, the application of privacy and data protection rules to research has reached higher attention in media, institutions and in the academic arena, although the topic seemed to be not adequately discussed in literature so far, unless few but relevant exceptions in the last months. This is why the need to further analyse this topic is even more pressing today. This special issue of Computer Law and Security Review has this goal: investigating on rules, potentialities and open issues of data processing for research purposes.

---


https://doi.org/10.1016/j.clsr.2020.105431

0267-3649 © 2020 Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license.
(http://creativecommons.org/licenses/by-nc-nd/4.0/)
The entry into force of the GDPR has given much more relevance to the issue of data protection in the field of research. The notion of research is now explicitly mentioned as an exception to the prohibition of processing of special categories of personal data (Article 9(j)), but also as an exception to the purpose limitation principle (Article 5(1)(b)), to the storage limitation principle (Article 5(1)(e) and as a possible derogation from some rights (right to access, rectification, restriction and objection). These exceptions, however, are counterbalanced by specific safeguards to be adopted in case of research purposes (Article 89). As also the preamble reveals, the GDPR recognises and encourages the development of scientific research⁷ (and this is why it provides specific exemptions to the general limits of data protection principles and rights), but with alternative suitable measures that need to be respected. Such measures may include specific transparency safeguards, simplified exercise of data protection rights, security measures and an attentive analysis of the impact of research on data subjects. In other words, one of the most relevant principles that researchers should take into account is accountability (see Ben Wagner in this special issue). Notions like data protection by design and DPIA becomes thus central. In general terms, we can affirm that there is a sui generis protection for the processing of personal data for research purposes.⁸

However, many issues are still unsolved, e.g.: how can we delimit the notion of “research” avoiding abuses of such terms as a legal ground for data processing? How to adequately protect research subjects, in particular the vulnerable data subjects? Should we consider consent as an adequate legal basis for processing data for research purposes or, to the contrary, it is highly unlikely that research subjects (including the vulnerable ones) might give a really “free” and unbiased consent? How could we enhance transparency in practice? What is the role of the accountability principle (including DPIA) when dealing with data processing in research and how such principle should interact with the principle of “ethics in research”? This special issue of CLSR will try to engage in discussions on these fundamental research questions.

The definition of research is vague and broad in the GDPR, since – as recital 159 explains – it should include also “technological development and demonstration, fundamental research, applied research” and even “privately funded research”. This might pose several interpretational issues, including e.g., defining the borderline between marketing studies and private researches; or between academic expression and scientific research,⁹ between medical treatment and health research, which is a timely problem in the age of coronavirus pandemic.

Interestingly, the EDPS has tried to delimit more the notion of research, to the cases with the aim of growing society’s collective knowledge and wellbeing, as opposed to serving primarily one or several private interests.¹⁰ But this notion seems still relative and open to discussions and interpretations (see Rossana Ducato in this special issue).

Another issue is what the exact relationship between law and ethics in research is (in particular in case of Coronavirus-related researches):¹¹ recital 33 argues that the provision of consent should be allowed also in case of undefined purposes, but only when “recognised ethical standards for scientific research” are respected. Interestingly, this is the only reference to ethics in the GDPR,¹² despite the broad discussion about data ethics in the European literature (see Charles Raab in this special issue).

Consent and purpose limitations are indeed two key issues that are largely addressed in this special issue, in particular in some critical areas of research, like genomic research (see Dara Hallinan in this special issue). The EDPB has already been very critical to the large use of consent in data processing for research purposes, in particular in case of medical trials.¹⁴ Research subjects are often in a situation of power asymmetry (patients, employees, asylum seekers, etc.) that generates decisional vulnerability.¹⁵ Such vulnerability does not allow them to give a really free consent according to Article 7 GDPR. This is in line with large part of legal literature in the field of data protection that recommends limiting the use of “consent” as a legal basis due to its fallacy and the difficulty to reach a really informed and free consent.¹⁶ However, the EDPS seems to generally accept the use of consent in the research

---

⁷ See, e.g., the tone of recital 159.
⁸ European Data Protection Supervisor (n 5) 21 referring to the ‘special regime’ for scientific research in the data protection framework.
⁹ ibid 9–10.
¹⁰ ibid 13.
¹² The only other indirect reference is: “breach of ethics for regulated professions” at Article 23(1)(g).
field, although at some specific conditions.\textsuperscript{17} The problem of using alternative legal bases are at least two.

First, while private universities or research entities can use “legitimate interests” (Article 6(f)), public universities or research centres would be forced to use “public interests” (Article 6(e))\textsuperscript{18}: this might create unreasonable disparities between different entities that should however respect similar rules and ethical standards (e.g., private entities would be required to do the balancing test, while the public ones would not; in case the data subjects object to the data processing according to Article 21, public entities could profit from the exemption at Article 21(6),\textsuperscript{19} while private entities cannot).

Second, in case of processing of special categories of personal data, the only legal basis alternative to consent might be the necessity for scientific research purpose (Article 9(2)(j)), but that legal basis is conditional to the approval of a “Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific” safeguards. As the EDPS argued, many Member States have not yet approved these laws.\textsuperscript{20} Accordingly, researchers might not use that exemption and would be required to ask for explicit consent (Article 9(2)(a)), even though it might be inappropriate in case of power imbalance between researchers and subjects.

Actually, in the age of COVID-19 pandemic, most Member States have already approved emergency pieces of legislation that include also the processing of special categories of data for research purposes.\textsuperscript{21} However, as also the EDPB has clarified, these legislations should be strictly limited to the duration of the emergency at hand and prove necessity and proportionality of the derogatory provisions.\textsuperscript{22} The issue of necessity and proportionality is a key issue also in the implementation of the DPIA (Article 35(3)(b)).\textsuperscript{23}

Another relevant problem in data processing for research purposes, especially in the age of pandemic, is purpose limitation. As affirmed above, the risks (e.g. for personal data of people tested positive to COVID-19) of secondary purposes with significantly adverse effects on individuals (and on democracy in general)\textsuperscript{24} might be relevant. The principle of purpose limitation in research might be limited, but relevant safeguards (Article 89) should be implemented: e.g., pseudonymization, transparency and personalized safeguards for vulnerable individuals (see Denise Amram in this special issue). Each of these purposes, however, might be problematic.

As regards pseudonymised data in research, some commentators have posed interpretational issues in case the data are acquired without the identifiers from a research entity which has pseudonymised the data: can these de-identified data be considered anonymous for whom acquires them?\textsuperscript{25} Regarding transparency duties, more discussion is needed for particular personalised information and legibility requirements in case of research (see Arianna Rossi and Gabriele Lenzini in this special issue): there might be “secondary” data subjects (e.g. relatives of the genomic research subject) that are not informed\textsuperscript{26} or there might covert researches where disclosing information might be detrimental to the success of the research (but the GDPR cannot help, since there are no exemptions for data collected directly from the subjects, Article 13),\textsuperscript{27} or there might be particularly cognitive vulnerable subjects that would not understand standard information.

The issue of vulnerable data subjects seems particularly unexplored in the data protection framework (see Gianclaudio Malgieri and Jedrzej Niklas in this special issue): the perspective of data protection in research (and the related literature on research ethics\textsuperscript{28}) might be an opportunity to finally address this issue, which also WP29 touched upon (without clear explanation) in several parts.\textsuperscript{29}

This special issue is not aimed at offering clear answers, but clear problematizations of open issues. The aim is to open

\textsuperscript{17} European Data Protection Supervisor (n 5) 20.

\textsuperscript{18} Article 6(1) at its last sentence clarifies that public entities cannot use the legal basis of “legitimate interest” at Article 6(1)(f).

\textsuperscript{19} Article 21(6): “Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(2), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest”.

\textsuperscript{20} European Data Protection Supervisor (n 5) 23.

\textsuperscript{21} See, as the first case in the EU, the Italian Decreto Legge n.14/2020, Article 14.

\textsuperscript{22} European Data Protection Board (n 3) 2.


\textsuperscript{27} European Data Protection Supervisor (n 5) 21


a vivid discussion with scholars, policymakers, institutions and stakeholders in order to balance two fundamental values of our society, which are also strongly related: cultural and scientific growth and fundamental rights and freedoms (including privacy and data protection). The first without the second has little value.

Declaration of Competing Interest

No conflict of interest.

Gianclaudio Malgieri
LSTS, Vrije Universiteit Brussel, Belgium

E-mail address: gianclaudio.malgieri@vub.be