European Union
European Regional
Development Fund

Investing
in your future

Research Integrity:

Framework Requirements, Values and Principles of Action

Research under the GDPR: paradigm shift or business as usual?

Tobias Schulte in den Baeumen

"It is paramount to understand how the GDPR will change not only the European data protection laws but nothing less than the whole world as we know it."

Jan Philipp Albrecht, Vice-Chair LIBE, Rapporteur of the European Parliament on the GDPR (2016)

What is data protection?

- With the GDPR, the scope of data protection seems to extend to other domains, primarily to IT and Cyber-Security
- Traditionally, data protection is a legal concept that does not intend to protect data per se, it rather aims to protect the person behind the data
- That is why we talk about the „right to privacy“ as a source of data protection on a global scale, and about the „right to informational self-determination“ in Europe specifically.
- As we live in a data driven world, and as researchers and research subjects have rights under the law, we need to find a balance between those rights (“concordance”).

The Need for the GDPR

- For a piece of legislation that was primarily drafted in 1992 and 1993, the Directive 95/46/EC was incredibly successful. The Directive was basically drafted in the pre-internet era, and together with the complementary legislative acts, such as the ePrivacy Directive, it wonderfully coped with the technological change of the last 25 years.
- As a Directive, it was transposed into national laws of the Member States, which significantly deviated, creating in fact not one Single Market for the data driven economy, but small regulatory islands in the ocean of the internet.
- Initially the European Commission was hesitant to accept that the time had come to work on the next generation of the EU data protection law. Due to its immense economic impact the Commission was aware that this would create tensions.
- Research faced the same obstacles and hurdles like businesses under the Directive.

The Idea behind the GDPR

- The GDPR tries to re-enforce principles that were shaped in the first years of data protection law, specifically it builds on CoE 108
- The GDPR wants data subjects to regain control over their data, and to make informed decisions who shall process data for which purposes
- The GDPR tries to turn back the times, as we have seen an increasing commodification of personal data in recent years. The common business model of the digital age is “data for service”, e.g., in social media like LinkedIn.

The Principles behind the GDPR

- The GDPR sets out seven key principles:
  - Lawfulness, fairness and transparency
  - Purpose limitation
  - Data minimization
  - Accuracy
  - Storage limitation
  - Integrity and confidentiality (security)
  - Accountability
- Research benefits from important exemptions from these principles. However, these exemptions are subject to adequate safeguards (Art 89).

Research under the GDPR

- The GDPR follows the tradition of the Data Protection Directives and the national laws which transposed the Directive: the GDPR acknowledges and re-affirms the importance of research as a common good and driver for societal development.
- The GDPR has been widely criticized by researchers during its final drafting stages. Some researchers from the social and medical sciences saw it as the ultimate coffin nail to cross-border research within the EU and beyond.
- Looking at the text of the GDPR, one has difficulties understand these critics as the GDPR is clearly supportive of research.

Regulation vs National Law under the GDPR

- The policy makers could not find a „final“ agreement on two important topics: employment and research.
- Thus, in the field of research we do not really have a Regulation, but rather a mix of elements of a Directive and a Regulation.
- It is up to the Member States to define the safeguards needed, and to use the exemptions the GDPR offers. Member States are not legally obliged to use these exemptions.

Regulation vs National Law under the GDPR II

- An example from Recital 156:

Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

- As Member States are free to decide whether and how they use the exemptions, and as national courts will interpret the cases, we will see a very heterogeneous legal landscape over time, undermining the freedom of European research collaborations. We may even see a market for data driven research, e.g., researchers may involve Estonian universities more in H2020 projects if Estonia makes widespread use of the research exemptions.

Research Exemptions under the GDPR

- Research occupies a privileged position within the Regulation. Organizations that process personal data for research purposes may avoid restrictions on secondary processing and on processing sensitive categories of data (Article 6(4); Recital 50). As long as they implement appropriate safeguards, these organizations also may override a data subject's right to object to processing and to seek the erasure of personal data (Article 89).
- Additionally, the GDPR may permit organizations to process personal data for research purposes without the data subject's consent (Article 6(1)(f); Recitals 47, 157). In isolated cases, these organizations may be able to transfer personal data to third countries for research purposes, without any other transfer mechanism in place (Article 49(h); Recital 113).
- The GDPR adopts a "broad" definition of research, encompassing the activities of public and private entities alike (Recital 159).

Informed Consent under the GDPR

- The GDPR may allow the processing of personal data, but still the IC will be the most common vehicle used to set up a legal base for the processing of data as it respects the right to informational self-determination of research participants.
- The GDPR sets out the expectation that consent would not be appropriate as a legal basis under this legislation where there is an imbalance of power in the relationship between the controller and the data subject, e.g., where the controller is a university (represented by a senior member of staff) and the data subject is a student of the same faculty.
- As using students is very common in social sciences, life sciences and psychology adequate safeguards are needed which protect the freedom of students to engage in such research. The same applies to patients in a hospital etc.

Informed Consent under the GDPR

- Informed consent under the GDPR is „"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her“.
- Question: how would you handle data relating to more than one person? For example, you may ring a bell at someone´s house and obtain data relevant to everybody in the household.
- While research is to some extent exempted from the specific consent, there is still a lot of discussion whether and how researchers have to fulfill the transparency and information requirements under Art 12 to 14 GDPR.
- Notably, the GDPR appears to prohibit any deception or misguidance of participants. However, we see a lot of cases in Brussels from social sciences and psychology which do exactly this.

Secondary Use of Data

- Under the Directive, secondary processing for research purposes was permissible only if the Member States "furnish[ed] suitable safeguards" (Recital 29). Thus, the presumption was that a controller could not further process personal data beyond the purposes for which it was collected, unless the relevant member state had enacted legislation permitting such processing activities for research purposes.
- The GDPR reverses this presumption, creating an exemption to the principle of purpose limitation for research. Article 5(1)(b) states, "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes." Article 89 sets out the safeguards that controllers must implement in order to further process personal data for research.

Procedural and Technical Safeguards

- Art 89 gives some privileges to research, but these tend to be subject to appropriate safeguards. The nature and quality of these safeguards depends on the respective requirement of the GDPR, and it will depend on the cultural setting in the Member State. In countries with trust in the research community, like Estonia or the Scandinavian countries, different standards will apply compared to Germany or the Mediterranean countries.
- Safeguards, and in particular procedural safeguards are embedded into a concept of social adequacy.
- When it comes to technical safeguards, pseudonymization / anonymisation, access right restrictions, and the encryption of data are cornerstones of the concept. Overall, research will have to invest more time and money into IT Security and Cybersecurity. Researchers must understand the intrinsic value of IT security.

Data Retention

- Some of the most vivid critics of the GDPR were biobanking organizations, and other members of the research community collecting vast amounts of personal data.
- Looking at the base line requirements of the GDPR, that seems to make sense. The GDPR's data retention requirements merely implement the use limitation principle of the traditional CoE 108 approach: keep personal data only so long as necessary to fulfill the original basis for collecting and processing it - and no longer.
- Obviously, a duty to delete personal data proactively sounds like a horror show to researchers, and the GDPR clearly recognizes the need to deviate from the general rule. Rather the opposite, the GDPR fails to protect the reasonable interest of data subjects and allows Member State to set up research exemptions which undermine the right to ask for the destruction of personal data.

Rights of Data Subjects

- By default, research participants have all the rights of data subjects under the GDPR.
- However, Art 89 par 3 GDPR allows Member States to „provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 ….. in so far as such rights 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". With Art 15 this includes the right to obtain information on the processing of personal data, as well as the right to receive a copy of the data.
- The question whether and how Member States will make use of the exemption of Art 89 par 3 will be key to the broader question whether we see a research landscape in the EU which may be more divided and secluded than under the Directive.

Accountability and Burden of Proof

- When people in business talk about the GDPR, they tend to raise three issues: the end of free tracking and retargeting, the burden of proof and the enormous fines under the GDPR.
- The research community may also keep in mind the new upper ceilings of 20 Million Euro. One should not forget, even the behaviour of Cambridge Analytica built on data coming from research. It would be naive to believe that all researchers strive for the common good.
- In many ways, the research community is way behind the industry. Not only in the pharmaceutical sciences, but broadly in science, researchers appear not to be used to document all steps demonstrating compliance, and they seem not to be used to regularly review and monitor their compliance with all applicable regulatory requirements.

Codes of Conduct and Professional Guidelines

- The GDPR offers an opportunity that may also benefit the research community: the use of codes of conduct and certifications to provide guidance on the GDPR's requirements.
- Art 40 par 2: *„Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation".* Such codes of conduct and certification mechanisms must be developed with a supervisory body.
- While the concept of Art 40 was designed for industry, the mechanism would allow the research community to overcome the frictions and hurdles following from the inconsistent use of the research exemptions by Member States.

Research with Third Countries

- By default, all limitations regarding the transfer of personal data to third countries apply. On top of the legal base for the processing, additional safeguards are needed for the transfer, e.g., the EU Model Clause contracts. When it comes to the US, the Privacy Shield does not apply to research.
- Again, the GDPR offers research an important exemption despite the fact that research may also serve critical purposes, e.g., the use of AI research for military purposes: under Article 49(1), a controller may transfer data when *"necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject."* Recital 113 makes clear that "*the legitimate expectations of society for an increase of knowledge*" should be taken into account. However, there are some conditions to this …..

Research with Third Countries II

- The transfer may be based on this ground only if it is not repetitive, it concerns a limited number of data subjects, and “the controller has assessed all the circumstances surrounding the data transfer and has on the basis on that assessment provided suitable safeguards” (Article 49(1)). Moreover, the controller must inform the data subject as well as the data protection authority of the relevant member state of the international transfer.
- The exemption follows directly from the GDPR and is not subject to a national legislation. Still, there will be a huge difference in the EU when it comes to the assessment of the impact on data subjects, and when it comes to the interpretation of the terms. My gut feeling would be, don't try this in Germany.

Miscellaneous

- Some problems require further discussion and deliberations, including but not limited to the following:

I. A lot of data becomes identifiable due to technological progress. While the old informed consent of data subjects remain valid, such data often does not have any consent attached. While the GDPR seems to allow the processing based on the legitimate interest of the researcher, or some rules on the secondary use, this feels a bit odd and unethical to me.

II. When you are in business, you may talk about the upcoming ePrivacy Regulation just as much as about the GDPR. Despite the wide-spread use of data from social media in social and political sciences, this does not seem to be a topic in research. Some thoughts about the fruits from the forbidden tree would be needed.

III. How will we ultimately handle data coming from third countries to the EU which have not been obtained in accordance to EU legal standards? Is that again a matter of the forbidden tree? Shall we fund such research under H2020?

„Bad“ research

- Talking about all the exemptions which shall facilitate research, one may wonder whether researchers deserve this trust.
- Clearly, 99 % of all researchers do, but the 1 % which is critical needs to be addressed as well.
- Even with the GDPR exemptions, the European Union will not be the place to do high risk personal data driven research, and we will never be as „cheap“ and skilled as competitors in China, India or even Belarus.
- In some areas of research, e.g., non-human primates, we see an extensive outsourcing of research to countries with less stringent rules. The same may apply in the future to data sciences operating with personal data.

If data is the gold of the 21st century..

Summary & Conclusion

- Listening to this talk, I hope you will wonder why researchers complained about the GDPR.
- Bearing in mind that research is not per se good, and that research serves economic or political interests, the depth and breadth of the exemptions is astonishing.
- It is up to the research community to justify these exemptions. If the research community fails, it will be the duty of national data protection authorities and the Data Protection Officers of the universities and research centres to ensure that the core values and principles will be enforced.
- Data protection is increasingly an bureaucratic monster, and it is hated by many for this, the GDPR may either kill data protection, or (with a bit of common sense) it may finally operationalize the 1981 principles of CoE 108.

The preparation of this lecture has been supported by the European Regional Development Fund (University of Tartu ASTRA Project PER ASPERA).

Also by the EC project PRINTEGER (Promoting Integrity as an Integral Dimension of Excellence in Research), which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 665926

THANK YOU!