DRAFT EVENT REPORT

ISC seminar: The Impact of the EU's GDPR on Health Data and Health Research in Europe

Dublin, 3 March 2017

Date of this report: 13 March 2017

ISC
Intelligence in Science

Table of contents

ISC seminar draft event report

The Impact of the EU's General Data Protection Regulation on Health Data and Health Research in Europe

Summary of event proceedings

On 3 March 2017 ISC in Dublin organized a seminar entitled "Impact of the EU's General Data Protection Regulation on health data and health research in Europe". The seminar brought together around 40 participants from academia, business and industry, and government to discuss and better understand the implications of the General Data Protection Regulation (hereafter: GDPR) on conducting scientific research, specifically health research, and collaborations in the Irish context, as well as in the EU and globally.

Introduction

1. **Declan Kirrane, ISC,** welcomed attendees and speakers. He stated that the GDPR will have a major impact on how science will be conducted in the future. The aim of the meeting is to understand and assess the impact of the EU General Data Protection Regulation on Science. The Commission is currently working on its proposals for the upcoming 9th EU research framework programme and the legislative process will commence in 2018. It is therefore important that the new programme is cognisant of the impact of the GDPR, as the regulation was not designed with science and research in mind and there are many unintended consequences. Moreover, in the post-Brexit EU there is an even greater opportunity for Ireland to take a leadership role in global research.

2. **James Lawless TD, Fianna Fáil Spokesperson on Science, Technology and Research,** pointed out that although the Department of Justice has responsibility for the GDPR, it does not fit neatly into one specific Ministry. He also raised some practical challenges and the issue of unintended consequences of data protection legislation, citing the example of health insurance. The VHI purged all records of former members after their membership had expired by more than six months. However, subsequent legislation required proof of membership of a health insurance plan to be eligible for community rating health insurance, creating a major predicament for the VHI.

   He underlined the dynamic nature of the research community, which is defined both on mobility of researchers and data. The GDPR aims to harmonise data protection legislation across all Member States, although there may still be certain derogations that are subject to local interpretation. Ireland must have a clear position. The challenge presented by the GDPR include protecting the right to privacy, while meeting the needs of the research community; keeping no more than necessary or as little as possible; methods of gathering consent for processing information; the anonymization of data and understanding how approaches to this by the different Members States. There is also not a sufficient level of awareness at public policy level, as well as on the general public level. Public policy institutions have not yet made the leap in terms of preparing for the GPDP. He also raised the issue of competing rights stating that the approach must be proportionate. Right to privacy is not absolute and so the challenge is to reconcile privacy rights with the rights of scientific community. He pointed to the difficulty in predicting future usage and how researchers can determine that they are collecting no more than is necessary. He emphasised the importance of a code of practice that would determine how the regulation is implemented within scientific community.

Panel 1: Scene Setting

3. **Kurt Zatloukal, Medical University of Graz,** gave a presentation of the data controllers perspective and said that advances in data analytics are transforming medicine. However, this transformation demanded a trusted environment to handle data. Citing the Eurobarometer survey, he pointed out that 31% of Europeans believe that they have no control over their data. The GDPR is pivotal to providing a trusted environment for data and enabling the implementation of the Digital Single Market. The key changes in the GDPR include: the empowerment of data owners; protection in third countries; a common EU basis; and severe penalties for breaches (4% of global turnover or up to €20 million). The data subject is empowered by having the right to information on the processing of their data, easier access to the data, the right to data portability and the right to be forgotten. However, there are many challenges ahead for data managers: practical issues have not yet been specified or identified; there is a real risk of fragmentation at Member State level; there is no "grandfather clause" in the GDPR[1]; a myriad of major technological and managerial issues; and a limited timeline to prepare as 28 May 2018, from when on the GDPR will apply, is fast approaching.

4. **Cathal Ryan, Office of Data Protection Commissioner Ireland,** also pointed to the Eurobarometer where 31% of people feel they have no control over their data. He noted that people are beginning to take notice of privacy laws and are becoming less apathetic. Cyber security attacks on health data pose a real threat. The data is lucrative; he referred to the World Economic Forum, stating that the new data economy requires innovation in governance and regulation – which, in their view, the GDPR does addresses. The GDPR addresses issues such as privacy by design[2]. Codes of conduct to promote compliance with law do add value to the regulation (and should not be viewed as a tick box exercise). The GDPR acknowledges that data protection is not an absolute right (recital 4). Recently the European Court of Justice called for a common sense approach to data protection. Organisations have always had an ethical responsibility to manage their data. Health research and data protection are not diametrically opposed. The need to engender trust is central. Health research is in the public interest, but it is in the public interest that research methods respect privacy. Hence, trust at core of health research. The erosion of public trust in public bodies due to data protection issues has become an issue in recent years (for example, Irish Water). Give control and avoid becoming subject to civil actions. Time dealing with the issues.

5. **Jeanne Kelly, Mason Hayes & Curran**, referred to a cultural change to people's attitudes. Data subjects have human rights to control the information that is out there about them. The GDPR is a game changer. Research community is privileged as there are numerous exemptions as long in their favour as long as they exercise appropriate safeguards. This is very different to commercial companies which are very restricted by the purpose limitation requirements meaning data can only be used for the purpose for which it was collected. Researchers have more scope in this regard provided they have safeguards in place. Hence the GDPR has provisions that are favourable to researchers. Nevertheless, there will have to be structural changes within organisations in implementing GDPR. For example, putting in place Privacy by Design and Privacy by Default mechanisms on data collected. Organisations should document the processes involved. Privacy

[1] A ***grandfather clause*** (or grandfather policy) is a provision in which an old rule continues to apply to some existing situations while a new rule will apply to all future cases. Those exempt from the new rule are said to have grandfather rights or acquired rights).

[2] Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start.

impact assessments should be conducted as a matter of routine and companies will need a budget-line to implement. An over focus on the fines for non-compliance can lead to a form of paralysis or inaction. There are some small steps researchers can take to enhance compliance. Data protection and the GDPR is a cross organisational issue – impacting on the legal/financial/IT departments. It is not reasonable to put the onus for compliance on one person or department. If the data is truly anonymised, then it does not fall within the remit of the GDPR. However, very few data sets are truly anonymised to a "legal" standard. If matching can be done, even with effort, then it is pseudonymization rather than anonymization. Pseudonymized data does fall within GDPR, and must be treated accordingly. The GDPR also includes new methods for transferring data outside the EU.

6. **David Byrne, European Alliance for Personalised Medicine (EAPM),** said personalised healthcare is becoming an increasing feature of health policy resulting in the creation of data plans for personalised health care. Hence there is better use and reuse of health data. New technology is developing new cures for rare diseases. This better use of data has the potential to bring savings equivalent to the budget of medium size EU Member State. The GDPR is central to this. There were 4,000 amendments put forward to the GDPR and many were adopted. Article 35 – information on natural person includes unique identifiers, factors linked to the genetic identity of a natural person, location data etc.

   The GDPR acknowledges the need to strike balance between protecting patient and data collection. Recital 54 acknowledges that "the processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject" while ensuring that this should not result in personal data being processed by third parties (such as banks, employers, insurance companies). Article 17 deals with the right to be forgotten allowing for retention "in the public interest, scientific or historical research purposes or statistical purposes." The recital on scientific research purposes requires that the legitimate interests of society are taken into account in the processing of data for research purposes. Health data is not the same as that held on social media sites. Research community needs to look at how data can be pseudonymized. Secondary uses of data are often unknown at the time when data is collected. There is a need to foster trust to gain the confidence of those who share their data. Much work still needs to be done in that regard.

7. **Tríona McCormack, UCD,** offered a research performing organization's perspective and said that UCD's biggest collaboration is with Trinity College followed by the UK, the US and then rest of EU. Researchers are now working in data rich environments. It is the multiple layers of information in such data rich environments that leads to innovation. Working at a transnational level can be challenging as borders can create barriers to innovation. GDPR aims to boost innovation and harmonise research across EU. Moreover, she acknowledged the research community is privileged as it is not as bound by the same restrictions in regulation as the commercial sector.

   The privileged position of the research community highlights the need to be trustworthy. Interestingly, 65% of the public have trust in academic institutions. Academic institutions need to look beyond the research to the potential outcomes. For example, in nutrition, diabetes presents a major challenge. There is a need to work with corporations, but such collaboration presents new challenges. When does the research become the product? This issue hasn't been worked out yet but is central to the purpose and outcome of research. Researchers need to work with finance and legal teams in order to minimise risk. The only certainty is uncertainty. Hence there is a need for a strong code of conduct, which in her opinion is a very practical response to this.

Panel 2: Processing personal data under the GDPR

8. **Tjaša Petročnik, ISC,** provided an introduction to the session on processing the personal data by reminding that the GDPR has been built on a premise 'one continent – one law' and that, since it is a regulation, it does not require transpositions. However, in the case of processing sensitive personal data Member States may introduce new/further conditions, including restrictions. Additionally, in the case of processing personal data for research, Member States can provide derogations to data subject rights. The application of the GDPR will introduce an additional (national) layer in the legal framework for organizations to navigate. Organizations operating in the cross-border context in several EU Member States will therefore have to understand and comply with different regimes, even after May 2018, which may hinder the consistent application of the GDPR. She then offered an overview of the current Member States' context; for example, Germany seems to have done the most as in January they have presented the revised GDPR implementation bill. Meanwhile, the UK expressed they remain committed to the GDPR, even in the light of Brexit, as data sharing is essential.

6. **Brian Quinn, INTEL**, first explained that Intel is primarily a compute and communications platform provider for data solutions – platforms that allow data to managed in a secure, trusted and effective manner. Trust in data management is essential and people need to feel secure in the knowledge that their data is protected. Security is paramount, whose entrusted with data (including Researchers) may believe that they are compliant with data regulations but if there is a security venerability (back door) then all regulation will be broken. Overall GDPR should be viewed as a good thing for research. The EU needs to portray a positive image; Europe wants to continue be an open jurisdiction which welcomes and nurtures knowledge. The future we will see an ever increasing important of (data based) machine learning – many new ways to extract knowledge from data sets currently too difficult to programme. Moreover, the sharp trend is towards visual (video) data and artificial intelligence will be central to understanding and utilising this data as computers can self-learn from various datasets. This (video data) will be central in the research context, and positive regulation will be good for research. Ultimately, the GDPR is good for research in Europe. It presents a narrative beyond Europe that the EU is a good place for data research.

9. **Graham Love, Health Research Board,** asked if GDPR should be viewed as good or bad thing? He concluded that it can and should be viewed as good but there is a strong need to build trust in the research community and evidence to create policies. Researchers have the power to change people's lives. There is a need for local enabling legislation to fill in gaps and noted that the Department of Health has started to move on this. Secondly, with the enabling legislation in place, there will be a need to build a framework with a strong and demonstrable governance system based on ethical principles. The essence of research is collaborative. The duty to share information is just as important as the duty to protect patient confidentiality.

10. **Fionnan Friel, Odyssey Validation Compliance,** first pointed out that life sciences is a highly regulated sector, for them harmonization in application is crucial; otherwise there we will see increase in costs. He also referred to other regulations and GXP, such as those governing clinical trials and pharmacovigilance, as data protection impacts and comes into place here, too. Security is central to the protection of data. It is imperative to maintain the integrity of the data at all stages in the research. The data must be accurate and cannot be modified. Pseudonymization calls for balance between accuracy and pseudonymization. Privacy by design is now becoming more of an issue. There is a need to set out the systems in place: who is data controller/processer; what type of service

level agreements are in place; who owns the data; where is it stored. There is also a need for the Cloud to meet the GDPR requirements as 95% of cloud apps are not GDPR compliant.

11. **Dietrich Rebholz**, **Insight Centre for Data Analytics,** spoke of the importance of securing data which in turn enables data to flow more freely. The protection of personal data is important, and the misuse of data is very harmful. Genomic data available needs to be held securely. The entire process on the flow of the data needs to be secure and trusted. The provenance of the data is important. It is also important to note that not all data is relevant. Artificial intelligence is assuming a greater role in data analysis. Other issues include where data is stored – should data be held locally on a hospital/research cite in a data centre or a central store? Also, the issue is how is data distributed. The purpose of the data often determines where data goes but this can place a burden on medical systems. There is a need to track where data goes and to be aware of where or how it could be misused.

12. **David Harmon, Huawei Technologies,** first stated GDPR is long overdue. Last regulation came in 1990s and we can be sure it will not take 20 years for revisions of GDPR. Exponential growth of data over the next few years will bring great opportunities for society; equally, these opportunities will bring clearly defined responsibilities from a data protection viewpoint for companies that will be providing these new big data related products and services to their customers. Technology is changing fast and it is important that legislation/regulation keeps on top of changes. He emphasized it is not just the issue of information, but also of the manner to transfer data. Artificial intelligence is increasingly important in data analysis and will determine the manner in which the information is used. Security requirements will demand complex technical specifications and present new challenges/problems. Security breaches leading to private information appearing on internet or becoming publicly available will erode trust. Regulation is necessary and proof of compliance important for building trust.

    More governments globally are enacting or updating laws so as to strengthen how personal data can be used or processed. This is the case now in the context of the EU. Huawei Technologies already employs data protection officers in different countries across the world including within Europe.

Panel 3: GDPR: the impacts for health R&D and data for health

13. **Martin Curley, MasterCard,** has been involved in numerous projects on open innovation, smart city, transportation. He understands the need to regulate. In terms of health research, protecting patient confidentiality must be a priority. The global research society has resulted in increased life expectancy where up to 10 years are added to people's lifespan. The GDPR is both welcome and necessary but there are concerns that we are looking at it very late and are not prepared. He also stressed the importance of the EU Digital Single Market and regulating for innovators, not against. He emphasized that there are tremendous opportunities in healthcare and that we need to strike balance between the greater good and individual privacy.

14. **Tim Lynch, Dublin Neurological Institute,** pointed out that emphasis so far has been on clinical research, but clinical care has not been mentioned. He also referred to the sensitive balancing act between patient rights and patient care. A consultant evaluating treatment for a stroke victim has 30 minutes to decide on treatment. How can they ensure speedy access to patient's records and make decisions? The link between the research and care is pivotal; clinical care needs clinical research. He also said that in the case of personalized medicine how to interpret the data is crucial. Moreover, ageing disorders will require significant data, but, for example, how does one obtain

consent from a demented or even psychotic patient? He concluded that the GDPR is good legislation, but one that requires monitoring and local tweaks.

15. **Walter Kolch, Systems Biology Ireland & Conway Institute UCD,** contended that GDPR is a positive development. It is important to regulate data collection and ensure that there is strong application to back it up. There is a need to think about implementation of the GDPR. It does present several challenges for the research field. Moreover, as technology is constantly changing the regulation will need to be tailored to specific circumstances. Health sector is a fast moving field with transforming effects; there is a growing need of putting information together, which brings to front data protection challenges. Now, most of medicine is reactive, but with big data we could achieve more structured prevention. He exposed the need for secure, interoperable cross-border data exchange for the patient's benefit, as there is no one size fits all solution.

16. **Kurt Zatloukal, Medical University of Graz,** closed the panel discussion on the question of implementation. There is a need for a code of conduct for researchers as the regulation deals in general principles, whereas the code can refer to current state of affairs in a certain field. The Code of Conduct should be a flexible instrument. It must be approved by the national Supervisory Authority or Commission. The advantages to code of conduct are that once an organisation complies with code of conduct then they have no need to worry. The needs and interests of patients, experts, and public need to be balanced. It is important to emphasise that there is no one way to implement – there is no "right" way or indeed a "wrong" way, but rather what is accepted. Nevertheless, academia and industry codes of conduct must be well constructed, coordinated, and adopted by research institutions from the outset. In terms of scientific culture and research integrity he stressed the issue of trust is essential and training for researchers needs to be provided in this area.

Conclusions

17. **Emer Costello,** summing up noted that there were several common themes coming through in each of the speakers' inputs. The panellists acknowledged and generally concluded that the GDPR was a good and positive development and should be embraced as such. It has the potential to enhance the reputation of Europe as a centre of excellence for research. The GDPR is also an essential component of completing the Digital Single Market. However, there is concern about the lack of awareness among policy makers of the potential impact of the GDPR and therefore a general lack of preparedness. It was noted that the GDPR presented opportunities to Ireland in a post-Brexit Europe.

    Public trust was seen by all speakers as being paramount in the collection and use of data. This posed many challenges. While the research community was in a relatively privileged position vis à vis the commercial sector, as they have numerous exemptions, there is an onus on the research community to continue to earn public trust by keeping data safe.

    Notwithstanding the various exemptions or derogations granted to research data, the GDPR presents many challenges to the research community:
    - Complete anonymization is hard to achieve and if the data can be traced back then it is pseudonymization, not anonymization, which does fall within the remit of the GDPR.
    - Collaboration with commercial organisations is central to the successful application of the research. There is a blurring of the line between research and product which has implications for research derogations.

- The accuracy of data is central to the integrity of the research.
- Implementation of the GDPR provisions is not the remit of just one person or department. There should be a transversal approach within the organisation to implementation involving all relevant sections – R&D, IT, legal, HR etc. There will be costs involved in the correct implementation of the GDPR.
- There is a danger that the margin of maneuver afforded to the Member States within the regulation could lead to fragmentation.
- There may be many unintended consequences of the GDPR which have not yet been identified – many 'unknown unknowns'.
- Much of the discussion has focussed on data research related to clinical trials. Issues on data collection, storage, retrieval in relation to clinical care should also be considered.
- The rapid pace of advances in technology, particularly in the area of artificial intelligence, make it difficult to predict future uses for data. The purpose limitation principle of the GDPR could present difficulties in the future.
- Policy-makers/regulators should keep up with the pace of change in technology/research. The GDPR will need ongoing review and amendment.
- A strong code of conduct/ethics code will facilitate research organisations remain in compliance with the GDPR. Research organisations would have nothing to fear from the GDPR once they adhere to the Code of Conduct.

Despite the challenges presented by the GDPR, there was a strong consensus that the duty of the research community to share data is equally important as the duty to protect the data subjects' privacy. Striking the balance between the two will be central to the development of a thriving research community across the EU.

The General Data Protection Regulation[3] (hereafter: the GDPR) entails a modernized, single set of data protection and privacy rules across many sectors and is aimed at empowering the citizens as data subjects, as well as establishing legal certainty for business and innovation based on clear and uniform rules. The regulation will replace the data protection directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data), dating back to 1995. The fact that the new data protection rules are now a regulation rather than a directive means that they are directly applicable in every EU Member State. There are several provisions, though, that give the Member States an option for exceptions.

1. The scope of the regulation

The GDPR will apply following the principle of 'one continent - one law' to all organizations in the EU that deal with the personal data in the context of its activities, regardless of whether the processing takes place in the EU or not. Both data controllers as well as processors (those processing the personal data on the behalf of controllers) will now be subject to obligations under the GDPR. Furthermore, it will apply to processing of personal data of the subjects in the EU by the controller or processor not established in the EU, which processes personal data relating to offering of goods and services to the data subjects in the EU or monitoring of their behaviour, as far as it takes place in the EU.

2. Key elements of the regulation

Enhanced data subject rights: The GDPR gives the data subjects (i.e. the individuals whose data are being processed) more control over their personal data and introduces new and enhanced rights for citizens, namely the need for clear consent for data processing, the rights to rectification, to erasure and 'to be forgotten', the right to data portability, and restrictions on profiling. Data controllers are obliged to provide transparent and easily accessible information to data subjects on the processing of their data.[4]

Obligations for organizations: The GDPR introduces several novelties that organizations shall consider. The regulation reads that the controller will have to implement appropriate technical and organizational measures, such as pseudonymization[5], which are designed to implement the data protection principles (such as data minimization) in an effective manner and to integrate the necessary safeguards to meet the requirements of the regulation ('data protection by design and by default'). According to the GDPR each controller shall maintain a record of processing activities under its responsibility. If the type of processing is likely to pose a high risk to the rights and freedoms of data subjects, the controller will have to carry out a data protection impact assessment prior to processing. In certain cases, organizations shall to consult the national supervisory authorities before carrying out the data processing. The controllers are to notify without undue delay the supervisory authority on the event of the personal data breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons, and also to the data subject, should the breach likely to result in a high risk to their rights and freedoms. Organizations – both controllers and processors – will have to appoint a data protection officer on the basis of their professional qualities and, in particular, expert knowledge

[3] 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): http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN

[4] Source: http://www.consilium.europa.eu/en/policies/data-protection-reform/data-protection-regulation/

[5] Note that pseudonymous data is a subject to the remit of the GDPR, whereas anonymous data is in principle not.

of data protection law and practices and the ability to fulfil the tasks, specified in the Article 39, where the core processing activities require regular any systematic monitoring of individuals on a large scale[6].

Personal data transfers to a third country or an international organization are permitted under certain set conditions. The European Commission is responsible for assessing the level of protection given by a territory or processing sector in a third country. Where the Commission has not taken an adequacy decision on a territory or sector, transfer of personal data may still take place in particular cases or when there are appropriate safeguards.[7]

Application and enforcement: The implementation of the GDPR foresees, inter alia, establishment of the codes of conduct and certification mechanisms for organizations to demonstrate compliance to the GDPR. The codes of conduct are encouraged as a mean of contributing to proper application of the regulation. The codes may be prepared by associations or representative bodies for approval, registration, and publication by a supervisory authority, or - if data processing takes place cross-border - by the European Data Protection Board, with the European Commission declaring the general validity of the codes across the EU. The compliance to the codes shall be monitored, which may be carried out by accredited bodies.[8] The GDPR also recognizes the validity of the binding corporate rules, outlining the minimum requirements to fulfil in order to get the binding corporate rules approved.[9] One single supervisory authority and enhanced cooperation between the national authorities of the EU Member States are foreseen (see below), as well as increased fines for violations of the data protection rules: data controllers can face fines of up to €20 million or 4% of their global annual turnover. The administrative sanctions will be imposed by the national data protection authorities.[10]

3. Possible implication for the use of data for health-related purposes

The use of health-related data has a potential to affect the life of an individual in a significant manner, therefore such data enjoys higher standards of protection. In the Article 9 the GDPR prohibits processing of special categories of personal data, which include genetic data, biometric data, and data concerning health, unless the grounds further specified in the GDPR exist. Health data can, however, be lawfully processed even without (explicit) consent for the purposes of preventive or occupational medicine, diagnosis, provision of health or social care or treatment, management of health or social care systems, under a contract on the 'medical care' ground, or in the public interest for public health reasons[11]. The regulation allows for the Member States to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.[12]

The regulation does allow processing of sensitive personal data for the purposes of (scientific) research[13], which need to comply with appropriate safeguards, including safeguards to ensure respect for the principle of data minimization. Where an organisation can argue that the further processing of

---

[6] Source: http://www.hldataprotection.com/2016/01/articles/health-privacy-hipaa/the-final-gdpr-text-and-what-it-will-mean-for-health-data/
[7] Source: http://www.consilium.europa.eu/en/policies/data-protection-reform/data-protection-regulation/
[8] Source: https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/43--guide-to-the-gdpr--codes-of-conduct-and-certifications.pdf?la=en
[9] Source: http://www.lexology.com/library/detail.aspx?g=9724744a-0441-4f9a-9c66-9dcc781a4395
[10] Source: http://www.consilium.europa.eu/en/policies/data-protection-reform/data-protection-regulation/
[11] Source: http://www.hldataprotection.com/2016/01/articles/health-privacy-hipaa/the-final-gdpr-text-and-what-it-will-mean-for-health-data/
[12] Source: https://www.taylorwessing.com/globaldatahub/article-health-data-privacy-under-gdpr.html
[13] Legal experts believe that the notion of what constitutes scientific research is to be interpreted by data protection authorities in the Member States.

data is necessary for scientific research purposes, the regulation provides a qualified compliance framework so long as safeguards are implemented. The organizations processing data, relying on the base of scientific research, may in certain circumstances also 'override' the individuals' right to object to processing or the right to erasure.

While the GDPR aims to enhance individuals' privacy rights, it also recognizes the importance of research and innovation, providing exceptions for scientific, historical, and health research.[14] Therefore, the regulation was generally welcomed by the research community. Research-based organizations, however, expressed concerns regarding the potential risk of fragmentation deriving from the possibility of Member States' derogations regarding the use of data for research that may establish uneven conditions for researchers and pose challenges for research collaboration between and amongst Member States and globally.

4. The timeline and key actors

The European Commission's proposal for the reform of the data protection rules was published in 2012. After negotiations and readings in the European Parliament and the Council the GDPR was finally adopted on 27 April 2016, then entered into force on 24 May 2016 and will apply from 25 May 2018 after a two-year transition period. At this point it has to be noted that the implications of the regulation are still not yet fully known, therefore the period before May 2018 will be crucial in terms of establishing and understanding how the regulation will be implemented.

The (distributed) governance model will be built on three pillars: national data protection authorities, enhanced cooperation between the authorities, and the European Data Protection Board level for consistency[15]. As defined by the regulation, each Member State shall provide for the supervisory authority[16], namely one or more independent public authorities responsible for monitoring the application of the regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the EU. The GDPR introduces a 'one stop shop' supervisory and cooperation mechanism, meaning organizations operating in several Member States are primarily subject to authority of one lead supervisory authority for cross-border processing carried out by that controller/processor. For the consistent application of the GDPR throughout the EU, the supervisory authorities shall cooperate with each other and, where relevant, with the European Commission and the European Data Protection Board. The board, joining the representatives of all 28 independent supervisory authorities, will replace the Article 29 DP Working Party, an advisory body on the issues regarding the data protection, established under the Directive 95/46/EC.

[14] Source: https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/
[15] Source: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf
[16] The list of the data protection authorities in the EU Member States is available here: http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm