Doshi M, 'Are Exceptions to the Rules a Threat to Privacy and Effectiveness of GDPR' EJPLT.
Available at:
https://universitypress.unisob.na.it/ojs/index.php/ejplt/announcement/view/144

EJPLT
ISSN 2704-8012

Are Exceptions to the Rules a Threat to Privacy and Effectiveness of GDPR

MANAN DOSHI
Student of Law from O.P. Jindal Global University, India

Abstract
Almost every aspect of our modern lives revolves around the presence of some form of data; from social media to banks and retailers, all our daily aspects have invariably been linked back to data available on us. The dependency on the use and presence of data and the sheer amount of sensitive personal data being entered into the system daily and one; triggered by the introduction of laws and regulations on the use of that data. The European Union (hereinafter "EU") in 2018 observing major risk and a subsequent need to protect the personal data of all individuals, brought into force the General Data Protection Regulation (hereinafter referred as "GDPR"). This was introduced with the objective to not only protect the personal data from being jeopardized, but also placing significant constraints and restrictions on the manner in which said collected data is utilized, stored etc. GDPR standardized the data protection laws in a manner such that a layman would understand the manner in which his data was being utilized and also raise concern the moment they feel their rights are violated. GDPR covers several aspects of the data and places mandatory guidelines and regulations to be complied with by all corporations within the EU, one such aspect that we will focus on through this paper is Research, and more particularly scientific research.

Keywords: GDPR; privacy; personal data; data protection; EU; regulation.

Summary: 1. What is Research? - 2. What is Scientific Research? - 3. Why is Scientific Research Crucial? - 4. Could Research be an Exception to Fundamental Data Protection Principles? - 5. Extent of Data Minimisation permitted by GDPR. - 6. Scientific Research through the International Relations Perspective. - 7. Conclusion.

1. What is Research?

The General Data Protection Regulation,2016 distinguishes between two main typologies of research: namely, historical and scientific research. "Research purposes are pooled in Article 89 GDPR with neighbouring scopes, such as archiving in the public interest and statistics." [1] Although Historical research, scientific research, statistical and archiving purposes are not expressly defined in the body of the Regulation but spelt out in the recitals; and hold extreme importance not only from regulation perspective but also from the law enforcement perspective. The loss of data from scientific research is and the risk of the data possessed is necessary to be understood. Before we go any further, we need to understand what Scientific Research within the scope of GDPR really entail.

2. What is Scientific Research?

Scientific Research is one broad category of data which depends heavily on the collection and exchange of ideas, knowledge and information and its subsequent processing of the people in the EU. "Scientific research is, therefore, any activity aimed at generating new knowledge and advancing the state of the art in a given field." [2] This concept picks up importance and momentum from the European Commission and their guidelines on expanding on research. The European Commission has defined the objectives of the EU's research and innovation policies to be 'opening up the innovation process to people with experience in fields other than academia and science', 'spreading knowledge as soon as it is available using digital and collaborative technology' and 'promoting international cooperation in the research community.

Scientific research has been brought in to the GDPR through Recital 159 and not through the substantive provision of the law. Thus, the precise meaning

[1] Ducato R, "Data Protection, Scientific Research, and the Role of Information" (*Computer Law & Security Review* June 25, 2020) <https://reader.elsevier.com/reader/sd/pii/S0267364920300170?token=80BDC535F67212DF14ECF5BA4136446A5822BE28E21D4339638092E84AFD033E8C8D85CA31A226B1BB373861A9346F98&originRegion=eu-west-1&originCreation=20220822123254> accessed October 3, 2022

[2] Ducato R, "Data Protection, Scientific Research, and the Role of Information" (*Computer Law & Security Review* June 25, 2020) <https://reader.elsevier.com/reader/sd/pii/S0267364920300170?token=80BDC535F67212DF14ECF5BA4136446A5822BE28E21D4339638092E84AFD033E8C8D85CA31A226B1BB373861A9346F98&originRegion=eu-west-1&originCreation=20220822123254> accessed October 3, 2022

under Article 89(1) of GDPR which provides for the regulations on scientific research are ambiguous and unclear. The statutory provisions, encompasses a wide range of activities inter alia, the technological development and demonstrations of the applied research of public and private institutions. The ambiguity has led to the countries creating their own set of rules and regulations to effectively manage their situation. "In several countries within the EU, however, the precise meaning of Article 89(1) GDPR is disputed. One could argue, based on recital 156 and the location in Chapter IX, that Member States must introduce special legislation defining any required precautions."[3] The concern remains valid as the laws/rules/regulations are not uniform and cause hurdles and even further confusion. Article 89(1) of GDPR states that, "personal data processing for archiving in the public interest, scientific or historical research purposes or statistical purposes shall be subject to appropriate safeguards for protecting the rights and freedoms of the data subjects involved."[4] Essentially saying that despite scientific research being an exclusion to the general principle; it is something that cannot be unregulated and unrestricted as there is a humongous ethical constraint attached in doing so.

3. Why is Scientific Research Crucial?

"Scientific research is indispensable inter alia in order to treat harmful diseases, address societal challenges and foster economic innovation. Such research is not the domain of a single type of organization but can be conducted by a range of different entities in both the public and private sectors."[5] Scientific research thus serves a valuable function in a democratic society to hold powerful players accountable for their actions and to ensure that the welfare of the citizens is not adversely affected; this has grown in importance with the concentration of control over information flow in the hands of a few private global companies. Data protection obligations should not be misappropriated as a means for powerful players to escape transparency and accountability. Researchers operating within ethical governance frameworks should therefore be able to access necessary API and other data, with a valid legal basis and subject to the principle of proportionality and appropriate safeguards. When it comes to scientific research, the GDPR establishes a two-tiered system to allow for derogations from these rights. First, by explicitly using GDPR rules on the condition that protections are in place, which must include "technical and organisational measures," and second, through Member State law.

Research falls into the exception meaning that consent of the individual for the sample to be used as data later is permitted. The sort of power and

[3] Ducato R, "Data Protection, Scientific Research, and the Role of Information" (2020) 37 Computer Law & Security Review 105412 accessed on May 8, 2022

[4] Staunton C, Slokenberga S and Mascalzoni D, "The GDPR and the Research Exemption: Considerations on the Necessary Safeguards for Research Biobanks" (2019) 27 European Journal of Human Genetics 1159

[5] Quinn, P. Research under the GDPR – a level playing field for public and private sector research?. *Life Sci Soc Policy* 17, 4 (2021). https://doi.org/10.1186/s40504-021-00111-z

exception must be accompanied by strong governance and ethical monitoring, as well as continuing dynamic alternatives, have been recommended to enable the oversight of waivers of consent in the biobank practise. Thus, GDPR mandates the presence of certain safeguards in order for there to be ethical scientific research conducted, which normally is violative of the privacy and human rights of the individuals. Safeguards do not create a binding obligations and enforceable rules of law. The safeguards despite being broad and over-arching covering a litany of concerns all at ones are not exhaustive and fail to ensure that the rights are not violated in any manner possible. The safeguards under the GDPR applicable on scientific research are as follows: (i) exception to fundamental data protection principles; (ii) principle of data minimisation applies; and (iii) pseudonymization wherever possible.

4. Could Research be an Exception to Fundamental Data Protection Principles?

The global approach to human rights, protection of personal data and ensuring privacy of their own and their loved ones, is taking an ethical direction. People are becoming increasingly aware of their surroundings, their rights and the need to protect their data on the internet; whilst also understanding the impact that the data on the internet has and can have on their lives from a possible data breach or misuse of that the stored data. Ethical constraints present a harmony between the desires of the corporations and that of the society at large; in comes the concept of Biobanks. Biobank research is built on long-term, well-organized collections of data and samples that can be used for a wide variety of purposes. The collection although being done in a highly systematic and conditioned manner, does not completely solve the ethical conundrum as the storing and processing of the data poses a significant threat. Despite the ethical conundrums present it is one of the better ways of data collection and storage currently being used and favoured. "The GDPR establishes a presumption of compatibility between (secondary) processing for research purposes and the original purpose of collection".[6] In this sense recital 50 confirms that the data controller may reuse data for research purposes, relying on the same legal basis as the initial processing.

Ethical conundrum relating to the data in possession of the biobanks mainly arises out of the fact that the data can be reused at a later stage, and it is not very tricky to bring out the fundamental details of the sample. This fear takes us into the next safeguard proposed to be maintained by the GDPR, that being principles of data minimisation. Data collected for scientific research is extremely precise, sensitive and of personal nature; thus, playing a major role in determining several theories and concluding many unfinished theories. "The data processed for research purposes may be kept in a form which allows the identification of data subjects even beyond the period strictly necessary for the achievement of the purpose for which they were originally collected."[7] The data set available would help create a general understanding backed by the

[6] Article 5(1)(b) and recital 50 GDPR.
[7] EDPS, Preliminary opinion on data protection and scientific research, 6 January 2020, p. 23.

highly sensitive and detailed data that would provide too much personal and sensitive information into the public sphere. Thus, data that does not attach to any identity or person at all is useless data and can simply be removed from the database as it would not assist in achieving the intended objective of the scientific research. This exception is particularly relevant in the context of scientific research, since the storage is fundamental to allow the verification of research results. The lawmakers do not intend to narrow down the ambit of scientific research but rather go with, "The intention to dissuade unlimited storage even in this special regime, and guards against scientific research as a pretext for longer storage for other, private, purposes"[8]

The only way an ethical conundrum would come to a rest is by anonymising the personal data to make it unidentifiable. Anonymisation and making the data unidentifiable, might hide the personal identity and identifiable features of the person, but it would still expose the origin of the person and other such determining factors that have an important role to play for a life with human dignity; which is a fundamental right in all of the EU. Anonymisation has its own challenges associated due to the technical disadvantage that they create in the mind of the data subject. "Pseudonymisation and anonymisation adds an extra layer of complication that is difficult to track or gain access to after the data/sample has been collected as it is divided into another set of data via encryption and anonymisation, GDPR requires you to use them wherever possible and feasible."Among these figures processing "necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on 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 measures to safeguard the fundamental rights and the interests of the data subject"[9].

5. Extent of Data Minimisation permitted by GDPR.

GDPR attempts to ensure and come up with alternatives, that the corporations and data collectors mainly biobanks for research purposes can use, and not end up storing non-anonymised data and samples with them for eternity. Article 5(1) of GDPR allows for data collection and storage to the extent that the collection is proportionate and necessary to meet the objectives of the research. This proportionate collection of data and its utilization is termed as data minimization. "Data minimization refers not only to the amount of personal data gathered, but also to the extent to which it can be accessed, further processed, and/or shared, as well as the purposes for which it is used and the time it is kept."[10] Minimisation will reduce the scope and extent of the personal data that can be stored, making it slightly tricky to get hold of all the information freely from a single source; as prioritisation

[8] EDPS, Preliminary opinion on data protection and scientific research, 6 January 2020, p. 23.
[9] Article 9(2)(j) GDPR
[10] Hayes B, "Ethics and Data Protection - EC.EUROPA.EU" (*European Commission,* July 5, 2021) https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf accessed May 8, 2022

would become key.EU laws on data protection and storing of data for biobanks and genetic research are derived from The Convention on Human Rights and Medicine (also known as "Oviedo Convention"). A convention that led to the creation of an instrument which prohibited the misuse of innovations made in the field of science and biomedicine, that would protect human dignity, The convention is a non-mandatory legislation that is not ratified by majority of the countries and is simply laying down the requirements that the countries could choose to apply to their domestic laws.

The potential scope of research exemptions by directly invoking the GDPR are narrow than through the previously practiced principle as under the European Data Protection Directive, 1995; where Member State laws that allow further derogations and reducing the impact of the laws so created. These laws created regulations which stated that "not only is a data subject's consent not required for the processing of personal data for research, but the data subject can also be stripped of a number of rights and others rendered ineffective, leaving the data subject with only an enforcement mechanism." The sort of guideline/regulation as mentioned above is the exact reason why The Article 29 of Working Party, in its guidelines on consent, understood scientific research as a 'research project set up in accordance with relevant sector-related methodological and ethical standards.' Under this approach, only scientific research performed within an established ethical framework would therefore qualify as activities falling within the special data protection regime. This means that even if data subjects are made aware that their data is being processed for biobank research, they may not have the right to access information or even object to the research being conducted. The data subject has not been bestowed right to restrict the use of their data for research purposes or make any request to the data controller to erase the data. The powers are restricted "to merely lodging complaints and hoping the data protection authority would further look into the matter."[11]

6. Scientific Research through the International Relations Perspective.

Data protection has been the critical focus of many governments, yet there is also a growing need within governments to develop frameworks which effectively harness the data economy. Protection ceases to remain the sole data related concern for governments around the world, as the finer nitty gritty's are beginning to be extensively explored by governments. Aspects such as sharing of data, parties between which data is shared and the bigger ethical questions surrounding the data economy are gaining attention and being explored to great details. However, the exponential growth of the information technology sector, has made today's data protection a lucrative field having to contend with the legalities and regulations, but also with the growing politicization of the field.

[11] Staunton, C., Slokenberga, S. & Mascalzoni, D. The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks. *Eur J Hum Genet* **27,** 1159–1167 (2019). https://doi.org/10.1038/s41431-019-0386-5 accessed May 8, 2022

This is not only evidenced through high profile cases such as the Edward Snowden case, but also through the increase in big tech's lobbying and influence, mainly in the United States political system. Consequently, different blocs are being demarcated in the information sphere. Nation-states are increasingly viewing the technological/data frontier as the battleground for geopolitical contestation. However, a growing number of leaders have expressed concerns regarding the splintering of the data sector, as evidenced by the creation of a Sinosphere internet. Collaboration is indeed the need of the hour, especially considering the rapid and continuous growth of new sectors and the need to regulate the said sectors on an urgent basis.

Data protection has never had to contend with the regulation of live/tangible personal information, Biobanking is exemplary of the aforementioned dilemma with only a few sparse precedents (Diamond vs Chakrabarty, 447 US 303 {1980}) nation-states are trying to negotiate the ethical implications of biobanking as best as they can. Biobanking is not in any means restricted to the single intention/implication it is being provided and the intersection of biobanking and data protection has to contend with the growing politicization of data sharing and ensure no foul play occurs.

The legislation of the biobanking sector in Europe is rather interesting and largely controversial due to lack of sufficient knowledge, awareness and desire to tackle the problems. Since the EU is not a federal state, but a supranational state, it does not have an overarching governance structure that every EU country must abide by. EU's supranational character has a potent influence on the data privacy laws that govern the region. The regulatory frameworks seek their legitimacy and strength through their harmonization by EU member states, and indirectly create a single market. As a result, there is no single European legislation regarding data privacy and protection which indirectly applies to the field of Biobanking. Despite being present it is not a comprehensive legislation which specifically addresses the concerns raised by privacy, genomic databases and biobanking. The regulations and their governance is an interesting concoction of cooperation amongst member states, whilst still respecting the national sovereignty and ideals of member nations. According to Franz- Stefan Gady,[12] this has allowed the European Union to have a top-down regulation system with heavy government involvement. Its model of supranationalism has also ensured cooperation within member states. Although, Brexit threatened to damage the cooperative ethos within EU, decades of strong leadership by leaders such as Angela Merkel and current leadership under Emmanuel Macron has seemed to restore member state's faith in the EU framework as a whole, and strengthened their co-operative character.

The Council of Europe is an integral body seeking to achieve a greater unity between the members for safeguarding of interests realising the ideals and principles which are their common heritage and facilitating their economic and social progress. The Council is the authoritative power which dictates the entwined relationship of biobanking and data privacy. Unlike the EU, Council of Europe is an organization embedded within the strata of international law

[12] Gady, Franz-Stefan. "EU/U.S. Approaches to Data Privacy and the 'Brussels Effect': A Comparative Analysis." Georgetown Journal of International Affairs, 2014, 12–23. http://www.jstor.org/stable/43773645

making the rules binding obligations and duties of the member states to practice. The Oviedo convention of 1997 legislates the relationship between human beings and the healthcare system but does not get the desired attention to fulfil the aim for which the organization was enacted and law passed. That being said, the human rights convention and judgements of the ECHR are binding on the council of Europe's Member States, and have played an integral part in shaping privacy laws in Europe.

Directives have an impact on the manner and light in which people observe the principle and determines the impact of the directive and ratification of the same. Directive 96/9/EC and 2004/23/EC are important for ensuring the privacy of the users is not forfeited for the actions of any individual, group or member state. Directive 96/9/EC crucially protects the rights of authorship in the data and provides a sui general legal right. Directive 2004/23/EC is a directive which regulates the clinical use of tissues and cells, consequently having an impact on privacy as tissues contain personal data. The Directives together make the people aware of the manner in which their data was being used in a manner not in line with the Fundamental Rights and needed to be protected. The violation was very evident as the data that was for the bio medical purpose was being stored and circulated in non-anonymised and un-protected format that disclosed and stored more than what was necessary. The data gave way to information that was excessive. Despite Article 14 of ECHR specifically requiring the data available to be circulated to third parties in only untraceable and unidentifiable manner, such that the identity is not revealed. The provisions and rules within the framework constantly seem to clash with one another, with the eventual conclusion being that the data of the eventual user is compromised and the whole purpose of legislation and safeguard is lost.

The American approach to regulating biobanking is quite frankly interesting. Similar to the European legislation, the United States does not have a governance structure dedicated to biobank and genomic database regulation as a whole activity; the legislation solely focuses on one arm of the activity i.e., biobank activities The presence and sole focus of several actors on a single activity makes every move less effective and less all inclusive (all-inclusive in the sense that considering all directions). According to Heather L. Harell,[13] the number of actors governing the biobanking sector has made the regulation of the sector "Disjointed and largely and indecipherable". The issue is multiplied multifold by the fact that America is the world-leader in practice of genomic databases and storage of data related to the same. The manner of testing, storing and reproducing all derive their eventual effect across the world from the principles enshrined by the United States. Specimens and data are accesses mainly through a variation of a three access model. Firstly, publishing the data on an open-source website, open access allows unrestricted access to data to anyone. Secondly, providing access to approved researchers only, as controlled access is extremely restrictive and much easier to regulate and ensure that no data leaks occur. Thirdly, tiered access is a middle ground between the aforementioned models, setting restrictions based off donor consent, the content of the specimen or the use of the specimen.

[13] Harrell, Heather. "Biobanking Research and Privacy Laws in the United States" (The Journal of Law, Medicine and Ethics, 2016)

Biobanks have several regulatory hurdles to be tackled for them to practice what they are practicing. Biobanks are mandated to be approved by the Institutional Review Board (IRB), before researchers can access specimens. Furthermore, the NIH (National Institutes of Health) takes an interesting approach to data sharing, which is predicated on sharing rather than restricting access to genomic data. Privacy protections are a required part of NIH policy, which stores sensitive data and is ultimately a privacy concern. Interestingly, the NIH implies the model of informed consent; only if individuals provide informed consent, would their de-identified data be placed on a publicly available website. These privacy considerations, may also prompt certain biobanks to ensure the destruction of the specimen after their research has concluded and the data is of no strategic importance to the cause of the research.

The NIH policy also mandates that data should be de-identified based on both the Common Rule and HIPAA privacy rule. This has catalysed much of the confusion with regards to privacy in the American biobanking. Although the laws should ideally go hand-in-hand, these laws are not well aligned. The Common Rule is the primary human subject's protection regulation in the US. The Privacy Rule, protects individual against information harm, whilst allowing for a necessary flow of health information.[14] Applicability of the law is a point of contention as the common rule only applies to certain researchers and research activities based on the source of federal funding, whereas HIPAA's privacy rule only applies to covered entities with a role in the payment chain of healthcare claims.[15] Apart from national laws, states also differ on whether they have laws addressing health research in lines with privacy. IRB's have been given little guidance, in turn increasing the confusion for biobank based-research institutes and the regulations which would govern them. This casts a doubt regarding the exchange of data between the US and other nations, affecting the overall quality of the research and also providing an inconclusive scenario in the world. The research would include only people from the US, and any breakthrough would not be tested for at the initial stage for application to other parts instantly. The objective of the research would be to improve the standard of living or eradicating an illness, which would not be satisfied. The safe harbour agreement governs the exchange of data between the US and the EU. The invalidation of the agreement by the EUCJ[16] is exemplary of US's shady and confusing data protection laws. Informed consent has become increasingly controversial, and its further catalysed by clashing regulations. The recent enactment of the Newborn Screening Saves Lives Reauthorization Act by prohibiting research is in clash with the 21st century Cures Act abolishing the need for informed consent. The current regulations are heavily focused on identifiability as a metric of privacy in biobanking.

The privacy rules and the common rule, assumes a slight risk of harm to individuals from research using de-identified samples and data. Therefore, the current US regulatory system is pushing for further scientific advancement in

[14] HIPAA Privacy Rule vs Common Rule, Health.mil
[15] M. A Rothstein, "Research Privacy under HIPAA and the Common Rule," Journal of Law, Medicine & Ethics 33, no. 1 (2005): 154-159.
[16] Gibbs, Samuel "What is 'safe harbour' and why did the EUCJ just declare it invalid?" (The Guardian, 2015)

the field of biobanking, whilst encumbering the privacy of the researched individual. The current regulatory frameworks are both inadequate and confusing, emerging from the conflict of interests between the parties involved. In his analysis, Franz- Stefan Gady [17] correctly diagnoses the US approach to privacy as a "patchy" and "reactive". The scholar emphasizes that US privacy law relies on ideals of self-regulation, which provides private companies a wide leeway in their usage of personal data to test new business practices, which result in privacy violations. Although the US 4th Amendment is invoked as the foundational source of "right to privacy", the Cambridge Analytica scandal and the disregard for privacy exhibited by US based Big tech companies, illustrates the flawed and weak understanding of "privacy" in American regulations.

The defining commonality between the US and the EU approach to data protection in the biobanking sector, is the lack of an overarching privacy framework which adequately protects the rights of the researched participants, whilst managing a positive push towards scientific advancement in the field. This is an absolute necessity, considering the importance and scope of biobanking. One must not look further than the vital role genomic databases and biobanking played in dealing with Covid-19. The essential issue with current privacy structures, is its focus on de-identification. The dilemma with de-dentification stems from the fact that de-identification as a solution does not provide individuals with control over data, which is the inherent idea behind data privacy. Yaniv Elrich, [18] therefore proposes the use of trust-enabling techniques to create a solution in which both researchers and participants win. A bilateral consent framework is inspired by participant centred research and peer to peer marketplaces. Yaniv highlights the role of Uber as an established mediator which brews trust between the service and its user. However more importantly, nation-states such as the US and EU must consider their own position in the biobanking framework. By being two of the largest players in the sector, any governance structure adopted by the two will set the tone for governance structures around the world. Biobanking's exponential rise, must be balanced with a stringent and robust privacy framework on an urgent basis.

7. Conclusions.

Under Article 89(3) GDPR, where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Article 15 (right of access by the data subject), 16 (right to rectification), 18 (right to restriction of processing), 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing), 20 (right to data portability) and 21 (right to object) GDPR. The same conditions as provided under Article 89(2) GDPR also applies to these derogations. In other words, these derogations are only allowed when necessary for achieving the archiving purpose at stake, and when

[17] Gady, Franz-Stefan. "EU/U.S. Approaches to Data Privacy and the 'Brussels Effect': A Comparative Analysis." Georgetown Journal of International Affairs, 2014, 12–23. http://www.jstor.org/stable/43773645
[18] Elrich, Yaniv "Redefining Genomic Privacy: Trust and Empowerment" (PLOS Biology, 2014)

the exercise of the data subject's rights would render impossible or seriously impair the achievement of that purpose.