Conducting Share Plan Research in Compliance with the European Union General Data Protection Regulation (GDPR)

Prepared by Dr. Bill Castellano, Rutgers University, with a special thanks to Don-Tobias Jol and Wouter Seinen, Baker McKenzie, and Margaret Loughlin, Fidelity Investments and Danyle Anderson, Global Equity Organization

Table of Contents

Chapter I: Overview of GDPR

What does GDPR mean for research?

Terms and Definitions

Chapter II: Benefits of Conducting Share Plan Research

Chapter III: Ensuring Compliance with GDPR

Phase 1: Legal Basis for Collecting and Processing data

Phase 2: Collecting and Identifying Data for Research

Phase 3: Collecting & Analyzing Data

Phase 4: Reporting Research Findings

Phase 5: Data Protection & Data Storage

Phase 6: Responsibilities of Data Breach

Chapter IV: Recommendations for Conducting Share Plan Research

The GDPR Research Checklist

Step 1: Recognizing Controllers and Processors for Research

Step 2: Identifying Data

Step 3: Research Purposes and Goals

Step 4: Legal Basis for Personal Data Processing in Research

Step 5: Data Subject Rights

Step 6: Documentation for Data Protection

Step 7: Security & Personal Data Breach

References

I. Overview of GDPR

The General Data Protection Regulation (GDPR), adopted in 2016 and effective on May 25, 2018, is a statutory framework that is designed to provide the freedoms of natural persons by processing and controlling personal data with greater protection within the European Union. Any organizations that perform any activities which process or collect any personal information of European Union (EU) residents within or outside the EU need to be compliant with GDPR.

GDPR is a complex and multi-faceted set of rules and many concepts and terms in the regulation remain relatively vague and ambiguous, especially in consideration of the accountabilities and limitations of research entities. Due to the voluntary nature of academic research, many researchers and organizations may be overwhelmed by GDPR and choose not to conduct research impacted by GDPR due to its complexity.

In short, GDPR aims to regulate how personal data is processed in the EU, which includes collecting, processing, storing, deleting, transferring and using. And thus, researchers as well as organizations who "process" or handle personal data of EU residents must comply with the rules. Therefore, it is important for all parties involved in a research project to understand and be familiar with the nuanced legal terminology and concepts of GDPR when conducting share plan research. Researchers must assess their goals and the type of data they will be collecting and protect any personal data that may be identifiable. Not complying with GDPR can result in a financial penalty and reduce the credibility of the research by the public.

Most important, GDPR was not designed to impede share plan research, instead, the implementation of GDPR is beneficial for researchers by providing more secure ways of processing and protecting personal data. To help researchers comply with GDPR, the guidelines in this report will:

1. Address concerns that a company may have regarding their compliance with GDPR.
2. Educate companies who have misconceptions about personal data processing in GDPR.
3. Provide researchers and organizations with policies and terms to ensure compliance with GDPR when interacting with potential clients for data collection.

While GDPR is likely to be the most comprehensive and profound data protection legislation that has yet been implemented in the world, it is not the only regulation imposing constraints on personal data in effect currently. For the purposes of this paper, we will address exclusively the rules and regulations related to GDPR and their impact on global share plan research. However, we strongly advise researchers and organizations to carefully consider additional data protection regulations that may be applicable to their projects.

"Many researchers and organizations may be overwhelmed by GDPR and choose not to conduct research impacted by GDPR due to its complexity."

Terms and Definitions

Terms	Definition
Data subject (Article 4(1))	The natural person who is directly or indirectly "identified or identifiable" by processing personal data. In other words, data subjects are identifiable human beings whose information is being collected or processed by the research entity.
Personal Data (Article 4(1))	All information relating to an identified or identifiable individual (data subject). The information must "relate to" the identifiable individual to be personal data. There are many circumstances where personal data is hard to distinguish; researchers have the obligation to consider all the factors as to whether the personal data is sufficient enough to make it identifiable information. Personal data will be further emphasized and explained in the later article in III, Phase 1.
Controller (Article 4(7))	The person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data. A controller determines the purpose and the means of processing personal data. The controllers are decision-makers who are indispensable in determining the processing of personal data, and they need to pay the data protection fee unless they are exempt. Think of a controller as the primary research entity who decides how and why personal data (data subject) is processed.
Processor (Article 4(8))	The person, public authority, agency or other body which processes personal data on behalf of the controller. Unlike the controller, the processor has different obligations under GDPR. The Processor acts under the behalf of the controller. In other words, the processor would receive personal data from the controller (or a third party) and is given instructions by the controller on what data to collect. Think of a processor as a subcontractor or another study site for the primary research entity who only follows the instructions given.

II. Benefits of Conducting Share Plan Research

Ensuring the continuation of share plan research and the researchers' ability to collect data is vitally important to individuals, organizations, and society. There is a wide body of research that demonstrate the positive impact that effective share plan strategies have on employee engagement and commitment.

Research has shown that specific share plan strategies, such as ensuring no wage substitution, offering both short-term and long-term programs, including a separate retirement program, and offering equity as a grant or at a discount has the greatest positive impact on employee outcomes. Additional research has shown that those organizations that also have an "ownership culture" which entails sharing information with employees, empowering employees to be more accountable, offering more training and development, including employees in decision making, providing financial wellness education, and embracing a participatory management philosophy have both higher employee and organizational outcomes.

Research has also shown that organizations which offer effective share plan programs and create an ownership culture have greater strategic and financial outcomes including higher productivity, more innovation, and higher returns on equity (ROE). Lastly, there is research being conducted to assess the positive impact of broad-based equity programs on employees' long-term retirement savings, which can help reduce the growing global income and wealth divide.

Faced with evolving disruptive technologies and increased globalization, organizations and employees are experiencing unprecedented challenges. We are witnessing an economic transformation in which many companies and jobs are becoming obsolete, while entire new industries are created. Organizations need to attract and engage a talented workforce to help them navigate these tumultuous times. Employees need to develop new skills and be more self-reliant managing their careers and savings. There has never been a more important time for continuing conducting share plan research to help better understand how employees, organizations, and society can respond to these unprecedented challenges.

"We are witnessing an economic transformation in which many companies and jobs are becoming obsolete, while entire new industries are created. Organizations need to attract and engage a talented workforce to help them navigate these tumultuous times."

III. Ensuring Compliance with GDPR

Phase 1: Legal Basis for Collecting and Processing Data

This paper focuses on the legal basis for collecting and processing data when organizations and research entities conduct share plan research. It does not include commercial research or other research conducted by an employer. GDPR demands that data processing must be lawful, fair and transparent. Lawful processing means that data can only be processed for a clear and specific purpose, and that the controller can rely on one of the statutory processing grounds set forth in GDPR (see below).

Transparency requires that the controller document the purpose of the research in a clear, transparent and concise written agreement in a non-technical way. Organizations must align how they plan to use the data with their declared privacy policy. Within organizations, there should be a regular cycle of reviews of their privacy policy, at least annually, to ensure alignment with how data is actually used across an organization. Under GDPR, individuals have the Right to be informed about the collection and the use of their personal data. Individuals also have the Right to Access, meaning that the individuals have the right to request a copy of their data, and "other supplementary information."

How to make sure data collection and processing for company research is lawful?

All organizations must have a legal basis for collecting and processing individuals' personal information. GDPR establishes six legal bases and researchers must determine at least one of the six lawful bases before conducting research. The most commonly used processing grounds are (i) that the processing is necessary to perform an agreement with or on behalf of the individual, (ii) that the individual gave its consent for the processing at hand, and (iii) that the processing is necessary for a "legitimate interest" of the organization and the processing is not against the privacy interests of the individuals involved.

When relying on consent as the lawful basis for the processing of personal data, such consent must be: (a) asked on the basis of clear and comprehensive information, (b) freely given, and (c) irrevocable at all times. If these conditions are not met, the consent is not valid and hence the processing is deemed unlawful. The "freely given" element is particularly difficult when employee data is concerned, since the common view is that due to the hierarchic nature of employment relationships, the employee is generally not fully free to withhold its consent and have the guarantee that such refusal shall not have consequences. Researchers that do collect data on the basis of consent should hence be mindful that they should ask direct consent from the individual, rather than asking the organization (i.e. the employer) to seek consent from the individuals for the researcher.

Also note that for the processing of sensitive personal data (such as information about the individuals' health, religion, sexual orientation, union membership), consent should be "explicit".

When researchers use explicit consent as their lawful basis, it is important to keep the consent request separate from other terms and conditions and to update and refresh the consent to ensure continued compliance if necessary.

Academic researchers typically use explicit consent. However, aside from explicit consent, the other lawful bases for collecting and processing data according to Article 6(1) are contractual requirement, legal obligation, vital interests, public task and legitimate interests. Academic researchers may use legitimate interest by demonstrating there is a legitimate reason for collecting the data and must clarify the specific and clear purpose and outcome of the research.

Statistical and academic research is an activity which is recognized by GDPR as something that should be accommodated by the policy maker. It is clearly mentioned as an example of "legitimate interest-based" data collection, and there is even a specific exemption in GDPR for processing of sensitive data.

"GDPR demands that data processing must be lawful, fair and transparent. Lawful processing means that data can only be processed for a clear and specific purpose."

Phase 2: Collecting and Identifying Data for Research

To comply with GDPR, researchers must recognize the different categories of personal and statistical data.

Personal Data

The definition of personal data under GDPR includes "identified" and "identifiable data." In other words, personal data refers to any form of data which can be used to identify a natural person, including names, email address, IP addresses (dynamic IP addresses), cookies, etc. It is crucial for data controllers, in this case, research entities, to be aware of their GDPR responsibilities as the controller of the data, but also how to pass and control those responsibilities if sharing the data with third parties. This is particularly important when collecting any personal data and any personal information that can be linked to an individual including but not limited to physical, mental, psychological, culture, economic, social identity, or any generic information that is personalized. Researchers must be aware and acknowledge the fact that personal data is under the protection of GDPR and must ensure they comply with these regulations.

Personal Data Special Category

Under GDPR some personal data are considered "special categories" which are sensitive data that require special protection and require explicit consent. Examples of sensitive personal data include race, ethnicity, religion, sexual orientation, etc. However, it's important to be aware that sensitive data which may be important to a research study can be collected under special conditions. Article 9 of GDPR mentions that when data subjects have given "explicit consent" under the special category, the processing of personal data is not considered within GDPR.

Also, researchers who find sensitive data from Publicly Available Data (e.g. Facebook, LinkedIn Page) or "online identifiers" where these data are manifestly made public by the data subject are not under the purview of GDPR. However, if there are identifiable information of data subjects, GDPR requires that these individuals have the right of erasure of their data, and upon making such a request, organizations must process the request within 30 days.

What if the research information is de-identified?

Personal data for research purposes can be collected if the information is "de-identified. "Only identifiable information is under the scope of GDPR. Therefore, personal data that has been anonymized is no longer in scope for GDPR. GDPR Recital 26 defines anonymized data as a subset of modified data where the personal information is nowhere to be found or tracked, making it impossible to identify individuals. Examples of collecting anonymized data for a research study would be the use of analyzing employee survey responses by pay grades, job titles, and the like—provided that the size of the data set and the level of aggregation is sufficient to rule out the possibilities that an employee can be singled out. Aside from anonymous data, GDPR is not applicable to data of deceased individuals.

However, if the personal data collected are identifiable, research entities or third parties need to demonstrate a legitimate business need that collecting personal data is critical for the research and ensure all the security and GDPR procedures are in place. If following an assessment, a determination is made that the research can be successful without the need of personal data then the best route is to either anonymize or pseudonymize the data. Given many research studies do need to analyze data from multiple sources, e.g. data from employees linked to data from managers, the data would need to be "pseudonymized" in order to comply with GDPR.

GDPR states that pseudonymized data should be the foundation of a data controller's collection and storage practices. GDPR defines pseudonymization in Article 4(5) as the processing of personal data where the personal data can no longer be attributed without the use of additional information, provided that such additional information is kept separately and personal data are not attributed to an identified or identifiable natural person. In other words, pseudonymized data is a technique that helps to remove information in a dataset that identifies an individual. For instance, data is effectively pseudonymized when a data controller conducts research where only the first initials are shown to represent the names for data subjects. Other common forms of pseudonymized data include showing only the last 4 digits of social security number, etc. In order to comply with GDPR, data controllers must use safeguards like pseudonymization to minimize the risk of the data breach.

Statistical Data

Under GDPR the collection of statistical aggregate data is permissible including data of groups of employees, households, or business entities.

"Researchers must be aware and acknowledge the fact that personal data is under the protection of GDPR and must ensure they comply with these regulations."

Phase 3: Collecting & Analyzing Data

Research Purposes and Goal Settings

GDPR does not specify what research purposes and goals are needed for compliance other than requiring the need to state the research purpose and goals before collecting and analyzing data. However, the research subjects must understand the purpose and the goals for the collection of data, and understand who is the data controller and how the data controller may share the data, e.g. with a data processor, or other third-party vendors as stated in a private policy available to all data subjects. If a research university is the controller, then it needs to specify which personal information is to be collected, the legal basis for collecting and processing the information and clarify the purpose and the outcome of the research. Alternatively, if the research university is the processor, then the controller is likely to be a third-party sponsor and the university will need to comply with the controllers' stated obligations. A university can be simultaneously considered the joint data controller, i.e. controller and the data processor, if it is using its own data for conducting the research.

If additional data is needed to continue the research, then the data controllers (or research entities) need to further clarify the specific purpose for the collection of additional data. GDPR also requires researchers to specify the time frame for conducting the research. It's important to note, the consent form and/or privacy statement must indicate the expected length of the research and keep the data subjects updated about their personal data protection and processing.

Purpose Limitation

To comply with the principal of Purpose of Limitation under GDPR, researchers (data controllers) need to clarify the purpose and outcome of the research and disclose what personal data is being collected. GDPR states that personal data can only be collected for specified, explicit and legitimate purposes. But GDPR also states that further processing of archived data for continuing research in the public interest, scientific or historical research purposes or statistical purposes will not be considered incompatible with the initial purposes. To clarify, if the new purpose of the research is compatible with the initial purpose, then the controllers do not need a further lawful basis for data processing. On the other hand, if the research is not compatible with the initial purpose, then the controller needs to specify a new purpose of the research. The stated purpose must also note what appropriate safeguards will be used for personal data protection, e.g. encryption or pseudonymization. Furthermore, the controller needs to get individuals' specific consent for the new purpose. After all, being lawful, transparent and fair are always the fundamental basis for data processing in compliance with GDPR.

Data Minimization

Another "specific goal" that GDPR mentions is Data Minimization. According to GDPR, personal data must be adequate, relevant and limited to what is necessary for processing. Data controllers need to specify why the data is needed and relevant for the purpose of collecting and processing data, and how long will the data be stored. Most important, GDPR aims to prevent the collection of unnecessary personal information and minimize the time that personal data is stored to reduce the event of a data breach. The controllers are required to maintain the minimum amount of data to be considered lawful.

Right to Erase or Restrict Processing

In order for the processing of personal data to be more lawful, individuals have the Right to Erase, delete and be forgotten. The research entities have to stop using personal data in the research if the data subject wants to withdraw the consent and the information can either be deleted or anonymized (and from those of its third-party or third-party suppliers). Also, GDPR gives the individual the Right to Restrict Processing, meaning that individuals can limit the way that the organization uses their data. If the data is unlawfully processed (legal basis), individuals can choose to restrict the process.

Phase 4: Reporting Research Findings

The reporting of the research findings must align with the stated purpose and goals of the study. A best practice is to report all findings using aggregate data to prevent the possible identification of personal data. GDPR requires extensive managed processes and effective communication methods to protect individuals from the risks of re-identification.

Keep in mind, GDPR requires the Right of Access in processing and reporting research findings by individuals. Therefore, the controller must provide proof that the data is aggregated before reporting research findings to prevent the identification of individuals. Special care must be taken to explain how personal data is protected when communicating results to different audiences. However, the right to erasure must be kept in consideration: the controller may need to delete data upon an erasure request. If a data subject requests their data to be deleted or removed from the research, then this must be respected.

The best practice for documentation of processing activities can be found in The GDPR Research Checklist included in the Appendix to this report, which illustrates detailed steps as well as the documentation that the research entities need to be in compliance with GDPR.

Phase 5: Data Protection & Data Storage

To comply with GDPR, researchers (data controllers) need to indicate that any personal data is held in a single, secured, and verified database. The data controllers need to be aware of where the information is located and stored, who has access to the data, as well as how is the information being audited and processed. In order to minimize the risks of a data breach, the controllers need to take measures and raise awareness on the protection of personal data processing. GDPR under Article 35, states that additional protections are necessary if there is a high risk to individuals' personal data whereby a "Data Protection Impact Assessment (DPIA)" is required to ensure the integrity of the technology used in collecting and processing the data.

GDPR also emphasizes there must also be safeguards to ensure the security of the data when stored, analyzed and published. The safeguards must ensure that "technical and organizational measures" are in place to protect personal data and conform with the principles of "data minimization. "Examples of safeguards include establishing firewalls to prevent unauthorized access of data, converting the data using data encryption and pseudonymization, or storing data in a protected filing system.

Data encryption is a common way to protect personal data. However, it is important for data controllers to ensure the key to the algorithms used to convert data are also protected. As we introduced in Phase 1, pseudonymization is a key component of GDPR compliance and it is a safeguard similar to data encryption that can help to remove information that identifies an individual, reducing the risk of exposing personal data. Although GDPR does not illustrate the preference of the two safeguards method, both data encryption and pseudonymization can be used simultaneously to create better protection for data processing.

"If there is a risk, GDPR requires the controllers to report a personal data breach to supervisory authorities within 72 hours of noticing the breach."

Phase 6: Responsibilities of Data Breach

When a data breach is identified, the controller is required to review the impact of the breach on data subjects. The controller must report the data breach only when there is risk to the rights and freedoms of the data subjects. Thus, under Article 55 there is no need to report a data breach if the data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If there is a risk, GDPR requires the controllers to report a personal data breach to supervisory authorities within 72 hours of noticing the breach. Under GDPR, each country will have its own authority, for the UK the Information Commissioner's Office (ICO) will be the supervisory authority.

The report should include the nature of the breach, the number of data subjects affected, the contact information for the controller or IT personnel, the expected causes for the breach and the actions that will be taken. In addition, a communication informing data subjects whose personal data were exposed due to a data breach must be sent without "undue delay." The controllers shall communicate in a plain, simple and clear language to the nature of the personal data breach.

IV: Recommendations for Conducting Share Plan Research

The Global Equity Organization's (GEO) Academic and Government Council supports the spirit of GDPR in ensuring the protection of the personal data of employees who participate in employer-sponsored share plans. Given the growing importance of cyber security, all firms, whether operating in the EU or elsewhere, need systems and processes that protect individuals' private data. As a result, we expect similar regulations to be implemented globally. In fact, there are a number of privacy policies that share many of the features of GDPR.

Most important, all of these regulations do not in any way prohibit conducting share plan research. GEO's A&G Council actively encourages and supports the continuation of share plan research to create knowledge that helps its members understand the most effective share plan strategies that positively impact employee, organizational, and economic outcomes.

We encourage members to contact GEO's Academic and Government Council if there is interest in conducting share plan research. Our team can help you implement best practices to endure compliance with GDPR. Some of the best practices include:

1. Partnering with your internal legal, HR, and IT groups and Data Protection Officer (if your organizations has one) to ensure they are aware of how to conduct share plan research in compliance with GDPR.
2. Review the six legal bases for conducting research. Academic institutions typically require "explicit consent," which qualifies under GDPR. Academic researchers in partnership with issuers and/or service provides can also state the "legitimate interests" of all parties for conducting research, e.g. assessing impact on employee and firm performance. In addition, participating in research for the "public interests," e.g. assessing the impact on increasing retirement savings; also qualifies under GDPR.
3. Clearly communicate to research subjects the purpose and goals of the research and how long the study will last. Update your current privacy policy to allow for use of data for research.
4. Ensure the protection of subject's personal data. Research using aggregate data, data that is anonymized, e.g. using non-identifiable data such as salary grade, equity holdings, etc. are in compliance with GDPR. If personal data is required, then a data protection impact assessment is required to ensure compliance with GDPR processes and requirements.
5. Research that collects personal data can also be in compliance if its pseudonymized, e.g. using encryption techniques, or some other form of coding such as using employees' initials or non-identifiable IDs.
6. Consider who is going to do the research, e.g. the controller, sub processor, or vendor. Ensure all contract clauses are updated if the data is not anonymized. If personal data is to be transferred outside the EU, ensure you have control clauses within your contract/agreement that include all GDPR requirements.
7. Permit research subjects the ability to opt out of the research.
8. Report research findings using aggregate data.
9. Partner with your IT department to ensure all data is stored in a secure database. Consider deleting all data once its analyzed if there are no continuing plans to use the data for further research.
10. Partner with your IT and Legal departments to designate key individuals who are responsible for notifying authorities and/or research subjects in case of a data breach.

Overall, most research universities and organizations have processes and policies in place that comply with GDPR and typically do not prevent the use of data for research purposes. A careful examination of these policies should reveal a strong foundation for compliance and open the door for participation in share plan research projects.

On behalf of GEO's Academic and Government Council, we hope the information provided in this thought leadership paper will be useful to you and your organizations when planning and participating in share plan research. We strongly encourage you to consider introducing a share plan research project in your organization as we all look to actively substantiate the many benefits of employee share ownership.

Appendix: The GDPR Research Checklist

Step 1: Recognizing Controllers and Processors for Research

Controllers

- Collects and processes all data for the research.
- Decides the purpose or the outcome of collecting and processing the data.
- Decides which lawful basis to apply for the purpose of using the data for the research

Processors

- Are given the personal data by the controller or told what to collect. Note, if the processor is directly collecting personal data, then the processor becomes a controller, or at a minimum a joint controller
- Do not decide the lawful basis for processing, and do not decide the purpose of the data for the research.

Step 2: Identifying Data

- Identify if the data collected falls within the definition of special categories or statistical data.
- Identify if the personal data collected are identifiable or de-identifiable for the research.
- Determine whether the data collected need to be in compliance with GDPR (Anonymized data or pseudonymized data).

Step 3: Research Purposes and Goals

- Clearly state and document the purpose and goals of the collection and processing of data for research.
- Be open and honest about the research purposes and goals.
- Restate purpose and goals of any new research using collected data.

Step 4: Legal Basis for Personal Data Processing in Research

- Determine the lawful basis for collecting and processing the data.
- Document the legal basis for personal data processing.
- Continue the process for the original legal basis for data processing if the new purpose of the research is compatible with the initial purpose.
- Withdraw individual consent as soon as possible if requested.

Step 5: Data Subject Rights

- Communicate with data subjects concerning their individual rights. Provide information in a plain, transparent, lawful, concise, easily accessible and a clear language.
- Ensure data subjects understand there is no punishment or fee for requesting individual personal data be removed, deleted or rectified.
- Inform data subjects when and how long their data will be processed, and who to contact if they have a request or compliant.

Step 6: Documentation for Data Protection

- Document research processing activities in writing.
- Update documented information regularly and conduct monthly reviews.
- Record consent, personal data storage, research reports, data breaches, and any privacy notices.
- Record all legal bases, requests for individual rights and purposes of the research.

Step 7: Security & Personal Data Breach

- Have safeguards, like data encryption or pseudonymization, to protect personal data.
- If using a website, ensure there is a cookie policy and have a cookie statement available to all end users on the website.
- Conduct regular risk assessments to ensure ongoing protection of stored personal data.
- Limit the number of individuals who have access to personal data.
- Be knowledgeable of the responsibilities and required actions in the event of a data breach.
- Ensure to report any data breach within 72 hours of becoming aware of the data breach.

References

Guide to the General Data Protection Regulation (GDPR). Information Communication Office (ICO).
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

UK Research and Innovation. GDPR and Research – an Overview for Researchers.
https://www.ukri.org/files/about/policy/ukri-gdpr-faqs-pdf/

Information Commissioner's Office. Guide to the General Data Protection Regulation (GDPR).
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Acs, Gergely. Tresorit (Nov 22, 2017). Experts on GDPR #3: What is personal data under the GDPR?
https://tresorit.com/blog/personal-data-under-the-gdpr/

Eurostat. Your Key to European Statistics.
https://ec.europa.eu/eurostat/web/microdata/statistical-confidentiality-and-personal-data-protection

Intersoft Consulting. General Data Protection Regulation.
https://gdpr-info.eu/art-89-gdpr/

Etemadieh, Arianna. Nixon Law Group (June 11, 2018). The GDPR and Pseudonymization vs. Encryption. https://www.nixonlawgroup.com/nlg-blog/2018/6/11/guest-blog-pseudonymization-vs-encryption

Travis Greene, Galit Shmueli, Soumya Ray, and Jan Fell. Big Data. (Sep 2019). 140-162. Adjusting to the GDPR: The Impact on Data Scientists and Behavioral Researchers.
http://doi.org/10.1089/big.2018.0176

Shmueli, Galit and Greene, Travis, Analyzing the Impact of GDPR on Data Scientists Using the InfoQ Framework (May 23, 2018).
Available at SSRN: https://ssrn.com/abstract=3183625

Miranda Mourby, Heather Gowans, Stergios Aidinlis, Hannah Smith, Jane Kaye. International Data Privacy Law, Volume 9, Issue 3, (August 2019), Pages 192–206. Governance of academic research data under the GDPR—lessons from the UK.
https://doi.org/10.1093/idpl/ipz010

Johns Hopkins Medicine. Preparing for the EU GDPR in Research Settings. (May 22, 2018).
https://www.jhsph.edu/offices-and-services/institutional-review-board/_pdfs-and-docs/GDPR_Application%20in%20Research%20Settings.pdf

Maldoff, Gabe. IAPP (April 19, 2016). How GDPR changes the rules for research.
https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/