JYX JYVÄSKYLÄN YLIOPISTO UNIVERSITY OF JYVÄSKYLÄ

This is a self-archived version of an original article. This version may differ from the original in pagination and typographic details.

Author(s): Scheuing, Sachiko; Niininen, Outi

Title: GDPR guidelines for academic research in marketing

Year: 2022

Version: Published version

Copyright: © 2022 selection and editorial matter, Outi Niininen individual chapters, the contr

Rights: In Copyright

Rights url: http://rightsstatements.org/page/InC/1.0/?language=en

Please cite the original version:

Scheuing, S., & Niininen, O. (2022). GDPR guidelines for academic research in marketing. In O. Niininen (Ed.), Contemporary Issues in Digital Marketing (pp. 139-151). Routledge. https://doi.org/10.4324/9781003093909-17

13. GDPR guidelines for academic research in marketing

Sachiko Scheuing (https://orcid.org/0000-0003-0976-2151) Outi Niininen (https://orcid.org/0000-0003-3256-1075)

Corresponding Author: sachiko.scheuing@acxiom.com

The European Union General Data Protection Regulation (GDPR) has changed the level of rigour with which academics need to approach designing and executing research involving the collection of personal data. While the required care resembles that which is required by an Institutional Review Board, the particular areas on which researchers need to focus differ, and this is partly due to the nature of the data used when investigating how consumers interact with the marketing environment. In this chapter, the authors draw on their expertise in academic and commercial marketing research to propose a seven-step approach to designing GDPR-compliant research and provide an overview of the procedural and documentation requirements. The role of the institutional Data Protection Officer and how this person can assist in the process is reviewed, and examples of good practices are offered.

Keywords: GDPR; academic research; marketing; research design; compliance; Institutional Review Board

Introduction

With the introduction of the European Union (EU) General Data Protection Regulation (GDPR, 2016a, see Further Readings) and high penalties for failing to protect study participants' privacy, academic researchers must now design research that uses personal data with great care. The processes and documentation requirements for the GDPR are similar to what is expected by an Institutional Review Board (IRB) (Mourba *et al.,* 2019). While there are numerous publications on GDPR compliance for academic research in the medical field, little has been written about the lawful treatment of data for research in the marketing

context. This chapter attempts to fill this gap and suggests checklists that researchers can follow for designing GDPR-compliant academic research in marketing.

The topic of sensitive data will not be discussed in detail in this chapter; rather, the focus is on non-sensitive data. Data collection from secondary sources, including social media or third-party registries and databases, is also not addressed in this chapter because such data may be subject to further restrictive terms of use that are unique to each platform. Given that this chapter aims to highlight the impact of the GDPR on academic research, the debate on the intricacies of research styles is also omitted. Finally, this chapter relies heavily on legal articles, with the majority coming from the law text itself and regulators' guidance.

This chapter begins with an overview of IRBs, followed by a brief introduction of the GDPR and a description of the data used by academic researchers in the field of marketing. The chapter's second half includes a seven-step approach to designing GDPR-compliant research in marketing, including processes and documents that are required for a lawful marketing research project.

Institutional Review Boards seek to ensure ethical research practices

Academic research advances knowledge in society in general and thus often includes challenging research projects. Traditionally, IRBs have ensured high ethical standards for academic research. In the review process, the IRB's members review research proposals and all supporting documents, including instructions to study participants. Drawing on the national or institutional ethical conduct of research guidelines, this team of experienced researchers discusses the features of the proposed study. Researchers may then be asked to

provide further clarification of the project and/or adjust the research design. IRB approval is awarded only after the board members are satisfied with the ethical soundness of the research design (Ienca *et al.,* 2019).

Typically, IRB members review applications from psychological, medical, biological or physiological research projects. If the research aims to study respondents in vulnerable positions, IRB approval becomes essential. Furthermore, academics seeking external funding may also need IRB approval, even if their research does not involve human physiological data and is perceived as low risk. High-quality journals may also demand IRB approval before publishing a study (TENK 2019).

The responsibility for ethical research practice lies with all researchers, and typically only high-risk projects are taken through the full IRB review process. IRB processes can require a significant amount of time from even the most experienced researchers. Therefore, various processes for filtering out low-risk research designs that pose no challenge to the respondents' wellbeing or institutional reputation are implemented. Institutional research guidelines, example participant information packages and self-assessment for data management practices can be used to determine the risk level of each proposed research project. As an example, La Trobe University in Australia has developed a step-by-step online portal that allows researchers to self-certify projects with a low ethical risk (see Further reading).

In most instances, the GDPR mainly requests procedural changes to the already well-defined national codes for ethical research practice. Many research funding bodies and national-level

codes for the ethical conduct of research have now incorporated specific GDPR requirements (Meijering *et al.,* 2020; Tikkinen-Piri, Rohunen and Markkula*,* 2018).

The GDPR

In May 2018, the GDPR implemented a higher standard of data protection. The EU legislature believed that a stronger data protection law would give EU citizens more control over their personal data (see the European Commission Statement in Further readings). The GDPR is based on seven principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); and accountability.[1]

One of the important aims of the law was to harmonise the then-fragmented data protection laws of EU member states[2]. However, perfect harmonisation was not achieved due to delegated acts in the GDPR that allowed member states to supplement the law with additional national rules. Thus, even when working with research collaborators within the EU, some aspects of data protection requirements may differ slightly (Ienca *et al.,* 2019; Mourby *et al.,* 2019).[3] This chapter will focus on the uniform requirements in the GDPR that were adopted in all EU member states and the UK (before Brexit).

Designing GDPR-compliant research

[1] GDPR Article 5
[2] The GDPR 'where as' (3), (53), (150) and (152)
[3] GDPR Article 89(2)

The following section aims to help academic marketing researchers design studies that are GDPR compliant. It will also provide a general overview of the documents and processes that are required to treat research subjects' data lawfully. These seven steps are summarised in Figure 13.1.

<FIGURE 13.1 HERE>

As shown in Figure 13.1, the seven steps recommended to achieve GDPR-compliant academic research are as follows: review guidance notes already provided by your institution's Data Protection Officer (DPO); determine the applicability of the GDPR to the study (anonymous vs personal data); determine the legal grounds for processing data and whether a research exemption can be applied; study how data are analysed and utilised and if either results in profiling of the respondents; and identify whether there are instances in which the collected data may need to be shared with external organisations, including any cloud-based software that will be used for e.g. data collection or analysis.

Step 1: Review the documents provided by the DPO of your institution

EU regulators have long considered DPOs as key players in making organisations accountable for data protection.[4] Accordingly, the GDPR, a law that is based on the accountability principle, the role of DPO is clearly stipulated in section 4. If the university, institution or company of the researcher has appointed a DPO, they should be a valuable resource for the required research documents. The DPO's tasks include the provision of advice to the organisation and its employees.[5] DPOs can also help answer many of the

[4] Article 29 Working Party Opinion 3/2010 on the principle of accountability https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf
[5] GDPR Article 39(1) a

questions throughout the seven steps outlined in this chapter. Many academic institutions have already worked with their DPO to establish internal requirements for technical and organisational measures in academic research projects. These will be discussed later in this chapter under the section titled "Protecting personal data with appropriate technical and organisational measures".

Step 2: Determine the applicability of the GDPR to the research: Anonymous vs personal data

Before beginning a research project, it is important to determine whether the GDPR is applicable. The general interpretation is that if it is verifiable that the dataset does contain personal data, then the GDPR applies. The GDPR states the following regarding personal data:

> *Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*[6]

Thus, any information that can lead to a natural person or can be used to identify a person is considered personal data.

If data are anonymous, the GDPR does not apply to the research. Unlike personal data, anonymous data are not defined in the GDPR, but there are clues to what requirements need

[6] GDPR Article 4(1)

to be fulfilled for data to be classified as anonymous. Recital 26[7] of the GDPR states that data are anonymous only if the researcher, in their capacity as the Controller[8], is not in the position to either identify or single out the person with whom the data are associated. For instance, if the researcher has no means to (re)identify the research subject because he/she lacks access to the cross-referencing table, the data may be considered anonymous[9] (Mourby *et al.,* 2018).

Academic researchers, as medical researchers, often apply pseudonymisation techniques to protect the identity of research participants by replacing direct identifiers, such as names and addresses, with unique ID numbers (Verhenneman *et al.,* 2020). While pseudonymisation is considered a protective measure by the GDPR, pseudonymised data are still considered personal data; therefore, the law applies.

In the context of qualitative research, the researcher might unintentionally offer information that could lead to the identification or singling out of an otherwise anonymous interviewee. For instance, interviewees may be known for their exceptionally artful communications or even their vocabulary. Citing such respondents may result in the interviewee being identified if a quote is compared to the respondent's previous statements in the press or on social media (Ienca *et al.,* 2019). The paradox here is that it is often the most unusual, colourful quotes that bring true value to qualitative data analysis.

---

[7] Recital 26, for instance, provides a detailed explanation, which is provided in Article 4 of the GDPR.
[8] As defined in the GDPR Article 4(7)
[9] In Breyer vs Germany (C-582-14), the ECJ rules that anonymity is relative, meaning the same data can be personal data or anonymous data depending on the party http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=1130557

Aggregated datasets and organisations

When working with aggregated datasets (i.e. individual data are summarised or averaged for the entire group), on a geographic level, for example, such as for cities or street sections, data are considered anonymous (see the Future of Privacy Forum (FPF) Visual guide to practical data de-identification in Further reading). However, studying organisations' data requires further examination to determine whether the data are anonymous or personal. If employees are being studied, the GDPR will most likely apply. As an example, consider a data sample comprised of people with the title 'Head of the Purchasing Department' that does not include individual names but does identify companies. While the individual names are not known, it is likely that only one person holds this title per organisation, which means the data can identify a person and thus the GDPR applies.

If organisations' records are being studied but people and/or functions within the organisation are not, there are two possible scenarios. When the study includes only organisations with many employees, such as companies listed on the stock market, hospitals and universities, it is highly unlikely that a record will point to a single person; therefore, the research is likely not subject to the GDPR. However, if the study includes micro-organisations (i.e. a specific doctor's practice or a web store owned by one person), the data related to the organisation must be treated as personal data.

Step 3: Determine the legal ground on which to base the research's data processing

The GDPR requires that the processing of personal data, including for academic research purposes, be based on one of the six lawful bases provided in Article 6(1). For research in

marketing, consent and legitimate interest can be used as legal grounds (Maldoff, 2016 in Further readings).

Consent, which may be the most used legal basis in academic research, is a typical IRB requirement (TENK, 2019), although it has some limitations. The challenge lies in that consent must be specific and freely given[10]. Academic research processes do not always follow the original study plan, and the data analysis might eventually highlight a new direction for the study. Consequently, data use may fall outside the specific parameter communicated in the consent language (Ienca *et al.,* 2019). Therefore, when consent is used as a legal basis, the data must not be used for other purposes or other studies[11] unless, as we will discuss in the next section, GDPR exceptions can be applied.

When using legitimate interest, instead of consent, it allows data to be re-used in future research. To use legitimate interest as the legal ground for a research project, a careful written assessment that weighs the researcher's interest against that of the research subjects (i.e. a Legitimate Interest Assessment, LIA) must be carried out.[12]

Regardless of whether consent or legitimate interest is used, the legal basis must be documented and communicated to the research subjects when either legal ground is used.

Step 4: Determine whether a research exemption can be applied

[10] GDPR Article 4(11), also see GDPR Article 7(4) for examining whether consent is freely given
[11] GDPR Article 6(4) excludes data collected on consent from re-purposing.
[12] GDPR Article 6(4)

GDPR has provisions for certain scientific or historical research and for statistical purposes to be exempt from providing data subject rights such as right to data access, rectification, restriction, erasure and, in some cases, objection. In addition, the research can be exempted from purpose limitation, one of the basic principles of the GDPR that requires data to be used only for the purposes it was collected, and data retention limitation. Without these restrictions, the data collected for the research can be repurposed for future studies, even by other researchers.[13]

Marketing research that is aimed at improving products or financially benefitting an organisation will generally not be able to make use of the scientific research exception. By contrast, academic research by universities and research institutions is more likely to be considered scientific and thus able to use this provision. Marketing research that is carried out by academics for companies should therefore be examined with extra care to determine whether the provision can be used. If a study's results are summarised (e.g. in a report or academic publication) as opposed to being in a format that can be used for a people-based targeted marketing campaign, then the research may fall under the category of 'statistical research', which also enjoys the research privilege and the GDPR does not apply (see the Information Commissioner's Office [ICO] Registry of processing activities in Further reading).

Step 5: Determine whether profiling will be used as part of the research

While most research will carry out 'profiling,' as defined in Article 4(4) of the GDPR, it is uncommon for academic research to apply profiling followed by automated decision-making,

[13] GDPR Article 89, 17(3)d and 21(6)

which can have legal effects for the research subjects. In the academic context, profiling could include, for example, assigning a category classification to records, creating additional variables or enhancing records with additional information but without any automated follow-up processes that could prove detrimental to the study's participants. Thus, in most cases, the researcher does not need to collect explicit consent, which is detailed in Article 22 of the GDPR.

When it is determined that the exemptions of the GDPR are not applicable, additional requirements can arise when profiling is used. Such is the case when research results are then later used to make automated marketing decisions by a company (e.g. which advertisement message the research subject should receive). When applying the research data that are collected for marketing purposes, such as targeting particular groups of individuals with specific advertisements, research subjects must be provided with the opportunity to object to the marketing use of their data.

Step 6: Determine whether the research requires data sharing, the use of service providers and cross-border data transfer

There are instances when data need to be shared externally, including international research collaboration, the expectation to participate in Open Science, submitting an article for review to a top journal or completing externally funded research projects (Mourby *et al.,* 2019). Furthermore, some types of data transfer and data sharing are not obvious. For example, a simple career move by an academic could result in data being transferred between institutions and even countries (Mourby *et al.,* 2019).

When sharing data with research partners that require a Controller-to-Controller data transfer or working in a joint-controllership arrangement, a contractual agreement outlining the responsibilities and obligations of the research parties is essential, i.e. joint-controller agreement (Ienca *et al.,* 2019).

A data protection agreement that formalises the Controller-to-Processor relationship must be put in place when research partners are working on the researcher's behalf, under strict instruction or when a service provider, such as a survey platform, is used. The GDPR requires informing research subjects about the recipient or the category of the recipient of their data.[14]

Similarly, if the research data need to be transferred to countries outside the EU, it is important to ensure that the same level of data protection is granted to the data when it is transferred to a non-EU jurisdiction as would be used in the EU. Several instruments can be used; however, the most practical way is to sign a standard template agreement called Standard Contractual Clauses (SCC), which are drafted by the European Commission. Currently, there are two types of SCCs: Controller-to-Controller and Controller-to-Processor (or Processor-to-Processor). The Executive Vice President of the European Commission Margrethe Vestager has recently signalled that a new set of SCCs could soon be ready (Chee, 2020; Europa.eu 2020 in Further readings). The first type is suitable for data sharing with collaboration partners based outside the EU, and the latter is for cases that are working with service providers based outside the EU. When research data will be shared across borders, research subjects must be informed of the transfer.[15]

[14] GDPR Article 13(1) e
[15] GDPR Article 13(1) f

A recent ruling of the European Court of Justice (ECJ) requires additional protective measures when transferring data to the USA. This may be particularly relevant for quantitative marketing research because many internationally recognised online survey platforms are based in the USA (e.g. SurveyMonkey and Qualtrics). When using a US-based platform, the level of processing risk must be evaluated on a case-by-case basis, and a data protection agreement as well as an SCC must be implemented. One remedy may be adding contractual language to provide extra data protection. However, at present, neither the court ruling nor the European Data Protection Board has clearly defined this 'additional protection'[16] [17]. An alternative is to use a non-US platform, or even better, an EU-based online survey provider that does not transfer the data outside the EU, such as Webropol.

Step 7: Determine whether a Data Protection Impact Assessment is necessary

When increased risks are expected, a thorough review of the data processing via a Data Protection Impact Assessment (DPIA) becomes necessary. Processing is considered a high-risk task when, for instance, a systematic and extensive evaluation that can affect the data subject significantly takes place, sensitive data[18] is used on large scale, or the systematic monitoring of public areas occurs.[19] For example, a study that has surveillance cameras installed on billboard advertisements at major train stations would most likely require a DPIA.

---

[16] The ECJ's ruling on data transfer to the US, aka 'Schrems II' https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

[17] The EDPB's FAQ of the ECJ's ruling on Case C-311/18 -Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf

[18] Refers to a special category of data defined in Article 9(1): *Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*

[19] GDPR Article 35(3)

The GDPR details what information is required in a DPIA in Article 35(7). Some domestic regulators have also produced a DPIA template, and they are making these available through their websites.

Documentation and the processes required for a GDPR-compliant academic research proposal

The seven steps outlined in Figure 13.1. help determine whether (a) the GDPR applies to the research, (b) the research can make use of the GDPR exemption, (c) profiling takes place, (d) data will be shared and/or transferred to a non-EU country and (e) a DPIA will be necessary. The following section describes the documents and processes that are required to carry out compliant academic research in marketing.

Drafting the necessary documents

The following section guides researchers on the documentation required for GDPR-compliant academic research (see Figure 13.2.).

<FIGURE 13.2. HERE>

As shown in Figure 13.2. the GDPR has several requirements for supporting documents. Researchers must ensure that documents are written in a clear language that is easy to understand, demonstrate the completion of a legitimate interest assessment, include a privacy statement and a record of processing activities, document all measures aimed at protecting

collected data throughout the research process and, if required, complete the DPIA as well as plan how the study participants' rights to data protection can be implemented.

Use clear and plain consent language

If consent is being used as a legal basis, an explanation of the research processes needs to be written in clear and plain language. In addition, the consent language must be presented in a distinguishable form so that it cannot be missed.[20] Article 7(2) of the GDPR lists the requirements for capturing valid consent. Notably, for research subjects below age 16 years, parental consent is required.[21]

Complete a legitimate interest assessment

When the research's legal ground is legitimate interest, the researcher's interest in carrying out the research must be balanced against the interest, fundamental rights and freedoms of the research participants.[22] Only when the interests of the research participants do not outweigh the researcher's interest can legitimate interest be used as the legal ground.

The result of the balancing exercise, which is often called the legitimate interest assessment, must be documented. The Data Protection Network and the Information Accountability Foundation provide templates and guidance on how to carry out a legitimate interest assessment (see Further reading).

[20] GDPR Article 4(11)
[21] GDPR Article 8(1)
[22] GDPR Article 6(1) f

Write a Privacy Statement

Article 13 of the GDPR details the types of information that must be provided to the research subject. This information is typically provided as a Privacy Statement, either on a website that is specifically designed for the study or on the website of the researcher's organisation. It is also good practice to provide the information in layers. This approach helps when there is not enough space on the landing page of the online survey. In such cases, state (a) the purposes of the processing, (b) the identity of the researcher and (c) the participants' rights under the GDPR on the survey. The remaining information can be provided through a link to the Privacy Policy that connects to the website. When collecting data via interviews, the interviewee must be informed of any consequences that might occur unexpectedly and that could greatly impact the person in addition to (a), (b) and (c) above. The remainder of the information can be provided via email with a link to the privacy statement online (see Further Reading, 2016b).

Create a record of processing activities

The researcher's university or institution must keep a record of processing activities as defined in Article 30 of the GDPR. The researcher may be asked to provide information on the research subject's data and the processing envisioned for the study. Links to templates for the record of processing activities provided by the UK-Regulator, the ICO and a OneTrust translation of the Belgian document are included in Further reading.

Determine and document measures for protecting the collected data throughout the research process

Designing compliant research also includes implementing and documenting protective processes and measures for the data. Many of the processes listed in this section may already

be in place within the researcher's organisation, and the DPO may be able to help with fulfilling the data protection requirement.

Protecting personal data with appropriate technical and organisational measures

The GDPR requires organisations to implement appropriate measures to protect personal data. As part of a university or a research institution, the researcher will have access to technical and organisational measures and documentation that are already in place. The DPO or the IT and security departments may also be able to assist.

The higher the risk to the rights and freedoms of the data subjects, the more robust the protective measure the GDPR requires (risk-based approach). At a minimum, data pseudonymisation and encryption, robust systems and software, the ability to rapidly recover from a security incident and regularly tested security are expected, depending on the situation.[23] On the practical level, this translates to (among other things) only using software and apps that are approved by the relevant organisation's IT and security departments, regular installation of critical security updates, password protection of computers and laptops, the use of a Virtual Research Workplace with robust security measures and the pseudonymisation of data (Meijering *et al.,* 2020; Mourby *et al.,* 2019). The ICO has a comprehensive checklist for this purpose available on their website (see Further reading).

Carry out the DPIA

[23] GDPR Article 32

When the research is determined to carry the level of risk that triggers a DPIA, the assessment must be carried out and documented. Article 35(7) of the GDPR lists the assessment's requirements. The Commission Nationale de l'Informatique et des Libertés (CNIL), the French regulator, offers a comprehensive template and an app in both French and English that can guide the analysis (see Further reading). The institutional DPO may also be able to assist.

Plan processes to ensure research subjects' rights to data protection

If the research exception of the GDPR can be applied, the right to access, rectification, restriction and (in some cases) objection to processing are waived (Frauenhofer IOSB 2019). If the research is not exempt, the GDPR requires the implementation of certain processes to allow research subjects to exercise their rights to access, rectification, data erasure, restricted processing, data portability and the right to object. These are detailed in chapter 3 of the GDPR and summarised here in Figure 13.3.

< FIGURE 13.3. HERE>

Conclusion

The GDPR requires academic researchers in marketing to approach their data with extreme caution in a way that is similar to the IRB review process to ensure the ethical use of data in academic studies. Academic researchers in the field of marketing will be able to provide stronger protection to research data by using the seven-step approach for designing GDPR-compliant research recommended here. DPOs can provide invaluable help in generating the necessary documents and implementing research protection measures.

Key lessons for future research

- Research that includes personal data must consider and adhere to the rules of the GDPR.
- Research plans can identify the specific aspects of data protection that are applicable by using the seven-step approach introduced in this chapter.
- Researchers should complete the required research documents and processes in a compliant manner by using the results of the seven-step approach.

References

Frauenhofer ISOB, FH-Bielefeld (2019). *Leitlinien für den Datenschutz in der wissenschaftlichen Forschung zu Aspekten der Mensch-Technik-Interaktion,* Karlsruhe, Germany.

Ienca, M., Scheibner, J., Ferretti, A., Gille, F., Amann, J., Sleigh, J., Blasimme, A. and Vayena, E. (2019). 'How the General Data Protection Regulation changes the rules for scientific research study', by *Panel for the Future of Science and Technology*, ETH Zurich Research Collection, https://doi.org/10.3929/ethz-b-000391622

Meijering, L., Osborne, T., Hoorn, E. and Montagner, C. (2020). 'How the GDPR can contribute to improving geographical research', *Geoforum*.Pages 291-295

Mourby, M., Aidinlis, S., Gowans, H., Smith, H. and Kaye, J. (2019). 'Governance of academic research data under the GDPR—lessons from the UK', *International Data Privacy Law*, 9, 3. doi: https://doi.org/10.1093/idpl/ipz010

Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S.E., Bell, J., Smith, H., Aidinlis, S. and Kaye, J. (2018). 'Are 'pseudonymised' data always personal data? Implications of the

GDPR for administrative data research in the UK', *Computer Law & Security Review*, 34, 2, pp. 222–233. doi: https://doi.org/10.1016/j.clsr.2018.01.002

TENK the Finnish National Board on Research Integrity (2019). *The ethical principles of research with human participants and ethical review in the human sciences in Finland*, 3/2019, Helsinki, Tutkimuseettinen neuvottelukunta.

Tikkinen-Piri, C., Rohunen, A. and Markkula, J. (2018). 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies', *Computer Law & Security Review*, 34, 1, pp. 134–153. doi: https://doi.org/10.1016/j.clsr.2017.05.015

Verhenneman, G., Claes, K., Derèze, J.J., Herijgers, P., Mathieu, C., Rademakers, F.E., Reyda, R. and Vanautgaerden, M. (2020). 'How GDPR enhances transparency and fosters pseudonymisation in academic medical research'. *European Journal of Health Law*, 27, 1, pp. 35–57. doi: https://doi.org/10.1163/15718093-12251009

Further reading

Chee, F.Y. (2020). 'Revamped EU data transfer tool may be ready by Christmas', *Reuters*, 30 September, https://de.reuters.com/article/eu-privacy/revamped-eu-data-transfer-tool-may-be-ready-by-christmas-idUSL8N2GR5IU

Commission Nationale de l'Informatique et des Libertés (CNIL). 'Tool for data protection impact assessment'. The CNIL's DPIA tools are available on their website: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

Data Protection Network (2018). 'Template for legitimate interest assessment', *Guidance on the use of legitimate interests under the EU General Data Protection Regulation*: https://dpnetwork.org.uk/wp-content/uploads/2018/11/DPN-Guidance-A4-Publication-17111.pdf

European Commission: Statement by the European Commission on the GDPR. https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en#background

Europa.eu. (2016a). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

Europa.eu. (2016b). 'Guidelines for privacy statement': See pages 19 and 20 of Guidelines on transparency under Regulation 2016/679 by European regulators: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Europa.eu. (2020). 'Data protection - standard contractual clauses for transferring personal data to non-EU countries (implementing act)': https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries

Future for Privacy Forum (FPF). 'The visual guide to practical data de-identification' under 'aggregated anonymous': https://fpf.org/wp-content/uploads/2016/04/FPF_Visual-Guide-to-Practical-Data-DeID.pdf

Information Commissioner's Office (ICO). 'Checklist for technical and organisational measures': https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

Information Commissioner's Office (ICO). 'Registry of processing activities': A template of the ICO can be downloaded from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/ then choose 'documentation template for controller'.

Information Accountability Foundation (2017). 'Templates for legitimate interest assessment', *Legitimate Interests and Integrated Risk and Benefits Assessment*: https://b1f.827.myftpupload.com/wp-content/uploads/2020/04/Legitimate-Interests-and-Integrated-Risk-and-Benefits-Assessment.pdf

La Trobe University: Step-by-step online portal for self-certificating low ethical risk projects of La Trobe University, Australia: https://www.latrobe.edu.au/researchers/research-office/ethics/human-ethics

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

OneTrust: 'Registry of processing activities'. OneTrust has created an unofficial English translation of the record of processing activities created by the GBA: https://www.onetrust.com/wp-content/uploads/2017/09/Belgian-DPA-Registry-of-Processing-Activities-Template-20170907-EN.xlsx

Figure 13.1. Seven steps towards GDPR compliant research

Step 1	Review documents by the Data Protection Officer of your institution
Step 2	Determine the applicability of the GDPR to the research - Anonymous vs Personal Data
Step 3	Decide the legal ground on which to base the data processing for the research
Step 4	Determine if the research exemption can be applied to the research
Step 5	Examine if profiling will be used as part of the research
Step 6	Determine if the research requires data sharing, use of service providers and cross-border data transfer
Step 7	Determine if a Data Protection Impact Assessment is necessary

Figure 13.2. Guidance for the documentation required for GDPR compliant academic research

Use clear and plain consent language
Carry out a Legitimate Interest Assessment
Write a Privacy Statement
Create the Record of Processing Activities
Determine and document measures for protecting collected data throughout the research process
Implement the Data Protection Impact Assessment
Plan processes to ensure research subjects' right to data protection is guaranteed

Figure 13.3. Rights of research participants in the context of academic marketing research

Subject Access right
Research participants may request information of the data used in the research. The law requires the processing purposes, categories of data processed, recipients or categories of recipients of the data and where applicable the duration of storage and the criteria in determining the duration to be disclosed. In addition, a copy of the data must be provided to the research subject.[1]
Right to rectification
There may be occasions where research participants will request their data to be corrected, claiming that it is incorrect. In such cases, the researcher is required to make requested amendments without delay.[2]
Right to data erasure
The GDPR allows persons to request the deletion of their personal data. This right extends to data that were made public or shared with other researchers, which means data recipients will need to be informed of the deletion request.[3]
Right to restrict processing
Research subjects have the right to restrict the use of data about them, if (1) they believe the data about them is incorrect, for the duration for the researcher to verify the claim, (2) processing is unlawful but they do not want the data to be deleted, (3) data is no longer required for the research but they do not want the data to be deleted due to legal claims, or, (4) they objected the use of data for the research, for the duration for the researcher to verify if the objection has to be honored.[4]

[1] GDPR article 15
[2] GDPR article 16
[3] GDPR article 17
[4] GDPR article 18

Right to data portability
This right only needs to be considered in case the legal ground for the research is consent. There may be cases where a research subject requests the data that they have provided to be sent in a digital format. The research participant may, under certain circumstances, also request this file to be transferred to another organisation.[5]
Right to object
This right needs to be considered in case legitimate interest is the legal ground for the research. The research subjects may object to the use of their data, including profiling. Unless there are compelling reasons that demonstrates the importance of the research, that outweighs the interests of the research subject.[6]

[5] GDPR article 20
[6] GDPR article 21