SURVEYS · ETHICS AND LAW

GDPR and Survey Research: Lawful Bases, Consent and Data Rights

The European Union's General Data Protection Regulation governs how survey researchers collect and use personal data. This article explains which data it covers, the lawful bases for processing, when consent is needed, the rights of respondents and the special provisions for research.

ModQu research article · 833 words · 9 references (APA 7th edition)

The **General Data Protection Regulation** (GDPR) has applied across the European Union since May 2018 and, in a closely similar form, in the United Kingdom. It applies to organisations established in the EU and to those elsewhere that offer services to, or monitor, people in the EU. For survey researchers, it sets the legal rules for collecting, storing, analysing and sharing respondents' data (European Parliament & Council of the European Union, 2016; Voigt & von dem Bussche, 2017). This article summarises the main points; it is not legal advice.

What data are covered

The GDPR applies to **personal data**: any information relating to an identified or identifiable person. Survey data are personal data if a respondent can be identified directly, by name or email address, or indirectly, by combining characteristics. Online identifiers can count: the Court of Justice of the European Union ruled that dynamic IP addresses can be personal data when the holder has legal means to identify the user (*Breyer v Bundesrepublik Deutschland*, 2016). **Pseudonymised** data, where identifiers are replaced by codes, remain personal data. Only data that are truly **anonymous**, so that no one can identify individuals by any means reasonably likely to be used, fall outside the regulation (Article 29 Data Protection Working Party, 2014).

Some categories are **special category data**, including health, ethnicity, political opinions, religious beliefs, sexual orientation and trade union membership. Processing them requires an additional legal condition, and many surveys collect such data.

Lawful bases

Every processing of personal data needs one of six **lawful bases**, shown in Figure 1.

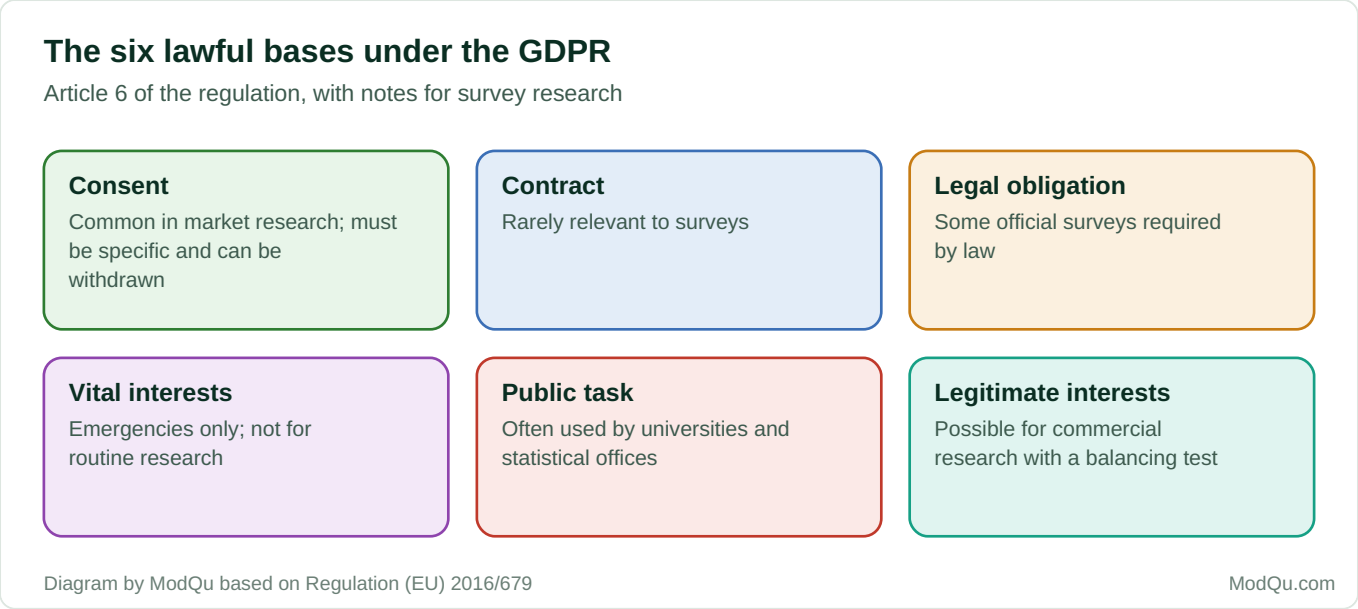


Figure 1. The six lawful bases for processing personal data under the GDPR and their relevance to surveys. Diagram by ModQu.

Three are most relevant to surveys. **Consent** is common in market research. **Legitimate interests** may be used by commercial organisations when processing is necessary, respondents would reasonably expect it and their interests do not override the organisation's. **Public task** is often used by universities and statistical offices carrying out research in the public interest.

When consent is the basis

Consent under the GDPR must be freely given, specific, informed and unambiguous, given by a clear affirmative action such as ticking an unticked box. Pre-ticked boxes and silence do not count. Respondents must be able to withdraw consent as easily as they gave it (European Data Protection Board, 2020). Consent for different purposes, such as taking part in a survey and being recontacted for future research, should be requested separately.

Legal consent is not the same as ethical consent to take part in research. A university may rely on public task as its legal basis while still asking for respondents' agreement to participate, as research ethics require (Mondschein & Monda, 2019).

Respondents' rights

Respondents have rights to be informed about how their data are used, to access their data, to have errors corrected, to have data erased, to restrict or object to processing and, in some cases, to receive their data in a portable form. Surveys must provide a privacy notice explaining who controls the data, the purposes, the lawful basis, how long data will be kept, who will receive them and how to exercise these rights.

Provisions for research

The GDPR recognises the value of scientific and statistical research. Article 89 allows some rights, such as erasure and objection, to be limited where they would seriously impair research, provided that appropriate safeguards are in place. Safeguards include **data minimisation**, collecting only what is needed, and pseudonymisation where possible. Data collected for one purpose may be used for further research without being considered incompatible, subject to these safeguards (European Data Protection Supervisor, 2020; Kuner et al., 2020).

International transfers

Many survey platforms and cloud services store data outside the European Union. Transfers of personal data to other countries are allowed only where the destination offers adequate protection, as recognised by the European Commission, or where safeguards such as standard contractual clauses are in place. Researchers should know where their survey platform stores and processes data before fieldwork begins.

Practical steps for survey projects

- **Identify the lawful basis** before collecting data, and record it.
- **Write a clear privacy notice** and link it from the survey invitation and first page.
- **Collect only what is needed**, especially for special category data.
- **Separate identifiers** from answers and delete contact details when no longer needed.
- **Set retention periods** and keep to them.
- **Use processors under contract**, such as survey platforms, with appropriate data protection terms, and check where data are stored.
- **Carry out a data protection impact assessment** for high-risk projects.

Professional codes, such as the ICC/ESOMAR code, require compliance with data protection law and set additional standards for respondents' rights (ESOMAR & International Chamber of Commerce, 2016).

Conclusion

The GDPR requires survey researchers to have a lawful basis for processing, to inform respondents clearly, to respect their rights and to protect their data. For research, it offers some flexibility in exchange for safeguards. Treating data protection as part of survey design, rather than a final check, keeps projects lawful and maintains respondents' trust.

References

Article 29 Data Protection Working Party. (2014). *Opinion 05/2014 on anonymisation techniques* (WP216). European Commission.

Breyer v Bundesrepublik Deutschland, Case C-582/14, ECLI:EU:C:2016:779 (Court of Justice of the European Union 2016).

ESOMAR & International Chamber of Commerce. (2016). *ICC/ESOMAR international code on market, opinion and social research and data analytics*. ESOMAR. https://esomar.org/code-and-guidelines/icc-esomar-code

European Data Protection Board. (2020). *Guidelines 05/2020 on consent under Regulation 2016/679* (Version 1.1). EDPB.

European Data Protection Supervisor. (2020). *A preliminary opinion on data protection and scientific research*. EDPS.

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union, L 119*, 1–88.

Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford University Press. https://doi.org/10.1093/oso/9780198826491.001.0001

Mondschein, C. F., & Monda, C. (2019). The EU's General Data Protection Regulation (GDPR) in a research context. In P. Kubben, M. Dumontier, & A. Dekker (Eds.), *Fundamentals of clinical data science* (pp. 55–71). Springer. https://doi.org/10.1007/978-3-319-99713-1_5

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer. https://doi.org/10.1007/978-3-319-57959-7