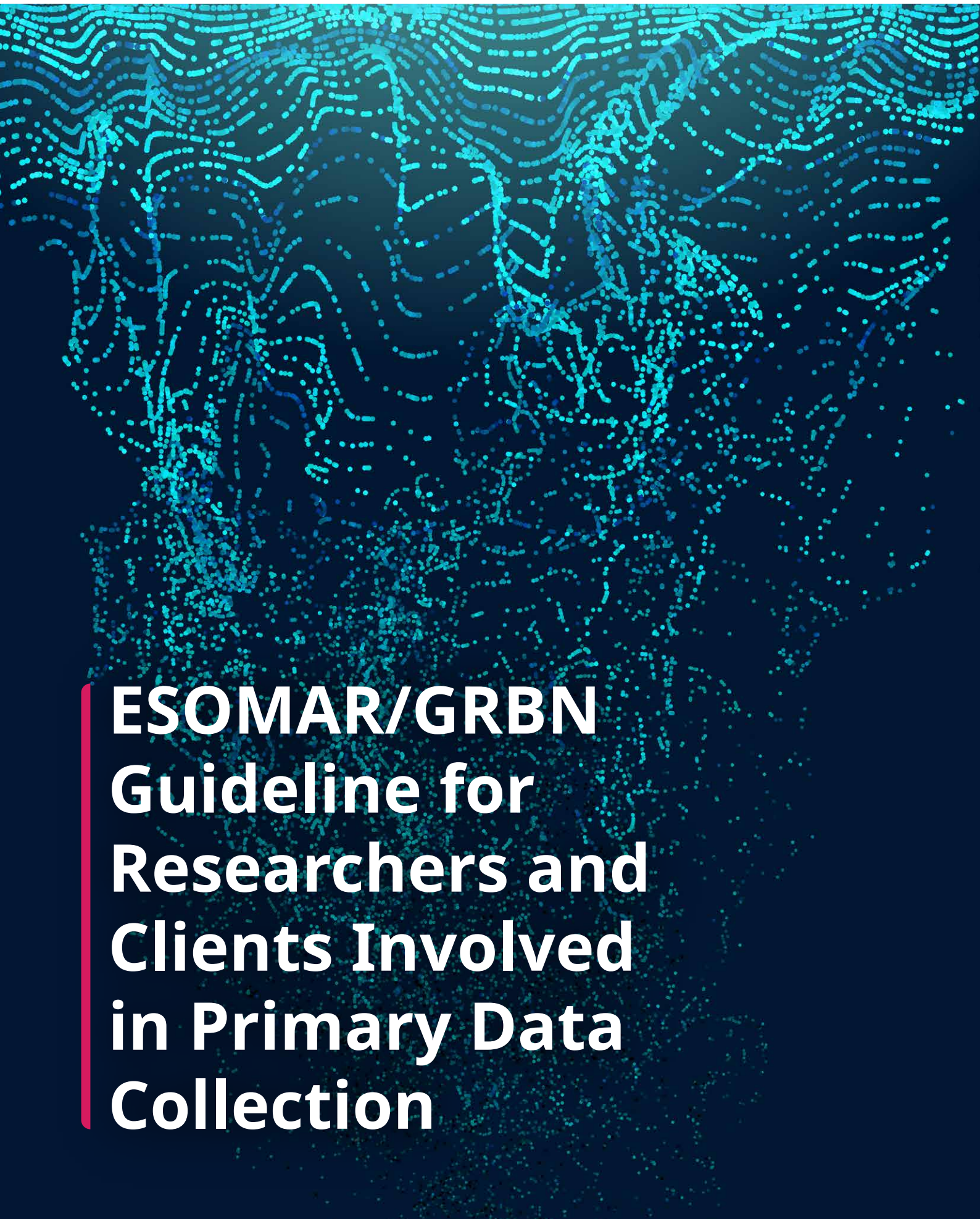
ESOMAR

GLOBAL RESEARCH BUSINESS NETWORK
APRC • EFAMRO • ARIA • AMRA



ESOMAR/GRBN Guideline for Researchers and Clients Involved in Primary Data Collection

Contents

1 Introduction

Decision-makers in all segments of society require a clear understanding of the environment in which they operate if they are to develop products, services, and policies that benefit their varied constituencies. Market, opinion, and social research and data analytics (hereafter "research") provides the data and insights needed for this evidence-based decision-making by commercial organisations, governments, non-profit organisations, and the general public. Often this requires the collection and processing of substantial amounts of data that can include personal data. In doing so, researchers and clients alike have a duty of care to those individuals (hereafter "data subjects") whose personal data we collect and process to protect that data, ensuring that that they do not experience adverse consequences or harms, as a result of having participated in research. These same protections apply when collecting data from companies and organisations of all kinds.

Researchers also have an ethical responsibility to decision-makers and other data users to be open and fully transparent about the specifics of the data collection and analysis. Such transparency is the only way for users of the research to judge its quality and determine whether it is fit for purpose.

2 Purpose and Scope

This guideline describes the ethical responsibilities of researchers, regardless of the type of organisation in which they work, when engaged in primary data collection, that is, when collecting data from or about a data subject for the purpose of research. It includes quantitative and qualitative methods that involve direct questioning of data subjects, but also methods of passive data collection in which the researcher observes, measures or records an individual's actions or behaviour. In all cases the key distinguishing features of primary data collection are (a) some direct interaction with data subjects (such as to gain consent) and (b) the purpose being research. Methodologies included, but not limited to, are surveys, focus groups, in-depth interviews, ethnographic studies and some forms of observational research, including mystery shopping. Its audience includes anyone conducting research in any setting.

This guideline also is meant to provide guidance for those who commission research to ensure that they are fully aware of their responsibilities and to set expectations about what is and is not possible given established ethical and legal requirements.

The requirements and best practices described herein are not meant to reflect the legal requirements of any specific country or region. Rather, they are designed to complement the ICC/ESOMAR International Code on Market, Opinion, and Social Research and Data Analytics, existing ESOMAR/GRBN guidance documents, and the codes and guidelines of national associations worldwide. As such, this guideline should not be consulted in isolation.

This ESOMAR/GRBN guidance does not take precedence over national law. Researchers responsible for international projects should take this guideline's provisions as a minimum requirement and fulfil any other responsibilities set down in law or by nationally agreed standards. It is not legal advice and should not be relied upon as such. It remains the responsibility of researchers to keep abreast of any legislation that might affect their research and to ensure that all those involved are aware of and agree to abide by its requirements.

Throughout this document the word "must" is used to identify mandatory requirements. We use the word "must" when describing a principle or practice that researchers are obliged to follow. The word "should" is used when describing implementation. This usage is meant to recognise that researchers may choose to implement a principle or practice in different ways depending on the design of their research.

3 Definitions

For the purpose of this document these terms have the following specific meanings:

Children

Individuals for whom permission to participate in research must be obtained from a parent, legal guardian, or responsible adult. Definitions of the age of a child vary substantially and are set by national laws and self-regulatory codes. In the absence of a national definition, a child is defined as being 12 and under and a "young person" as aged 13 to 17.

Client

Any individual or organisation that requests, commissions, or subscribes to all or any part of a research project.

Consent

Freely given and informed indication of agreement by a person to the collection and processing of their personal data.

Data analytics

Means the process of examining data sets to uncover hidden patterns, unknown correlations, trends, preferences, and other useful information for research purposes.

Data subject

Any individual whose personal data is used in research.

Harm

Tangible and material harm (such as physical injury or financial loss), intangible or moral harm (such as damage to reputation or goodwill), or excessive intrusion into private life (including unsolicited personally targeted marketing messages).

Mystery shopping

The use of fieldworkers, researchers or participants (consumers or general public) in the role of customers/users in order to evaluate a business/service performance.

Non-research activity

Taking direct action toward an individual whose data was collected or analysed with the intent to change the attitudes, opinions, or actions of that individual.

Passive data collection

The collection of personal data by observing, measuring or recording an individual's actions or behaviour.

Personal data (sometimes referred to as personally identifiable information or PII)

Means any information relating to a natural living person that can be used to identify an individual, for example by reference to direct identifiers (such as a name, specific geographic location, telephone number, picture, sound, or video recording) or indirectly by reference to an individual's physical, physiological, mental, economic, cultural or social characteristics.

Primary data

Data collected by a researcher from or about a data subject for the purpose of research.

Privacy

The right of an individual to be free from intrusion or interference and assumes that the individual has the ability to control, edit, manage and delete information about themselves, and to decide how and to what extent such information is communicated to others.

Privacy impact assessment (sometimes referred to as PIA or DPIA)

A process to identify and mitigate data subjects' privacy risks.

Privacy notice (sometimes referred to as a privacy policy)

A published summary of an organisation's privacy practices describing the ways an organisation gathers, uses, discloses and manages a data subject's personal data.

Research, which includes all forms of market, opinion and social research and data analytics

The systematic gathering and interpretation of information about individuals and organisations. It uses the statistical and analytical methods and techniques of the applied social, behavioural and data sciences to generate insights and support decision-making by corporations, governments, non-profit organisations and the general public.

Researcher

Any individual or organisation carrying out or acting as a consultant on research, including those working in client organisations and any subcontractors used.

Secondary data

Data that has already been collected and is available from another source.

Sensitive data ("Special Category data" in some jurisdictions)

Specific types of personal data that local laws require be protected at the highest possible level from unauthorised access in order to safeguard the privacy or security of an individual or organisation, and which may require additional explicit permission from a data subject before processing. The designation of sensitive data varies by jurisdiction and can include but is not limited to a data subject's racial or ethnic origin, health records, biometric and genetic data, sexual orientation or sexual habits, criminal records, political opinions, trade union membership, religious or philosophical beliefs. It can also cover other types of data (not necessarily legally defined) that can include location, financial information, and illegal behaviours such as the use of regulated drugs or alcohol.

Vulnerable individuals

Individuals who may have limited capacity to make voluntary and informed decisions, including those with cognitive impairments or communication disabilities.

4 Key Principles

Throughout the long history of market, opinion, and social research and data analytics researchers have recognized that individual data subjects have an inherent right to determine when and how their personal data is collected and used. To this end, research has been governed by three overriding principles:

- *When collecting personal data from data subjects for the purpose of research, researchers must be transparent about the information they plan to collect, the purpose for which it will be collected, with whom it might be shared, and in what form.*
- *Researchers must ensure that personal data collected and used in research is protected from unauthorised access and/or use and not disclosed without the consent of the data subjects.*

- *Researchers must always behave ethically, comply with all applicable laws and regulations, and not do anything that might harm data subjects or damage the reputation of research.*

These principles[1] form a foundation of trust on the part of the general public, whose data researchers rely on, and the clients who commission research to help them make better business decisions. They remain as important today as at any time in our long history.

Responsibilities to Data Subjects

5 Study Design

Researchers have ethical responsibilities to data subjects and fulfilling those obligations as members of a self-regulated sector begins at the design stage. Some guidance will be provided by the regulatory and data protection requirements of those countries where research will be conducted. However, there is considerable variation in regulatory requirements from country to country, with some being more restrictive than others. While researchers must be aware of and adhere to the laws in those countries where they collect or process data, meeting their ethical responsibilities requires more than simply complying with applicable laws. One effective way of doing so is through practices often described as "privacy by design."

5.1 Privacy by Design

The essence of privacy by design is implementation of a process that emphasises an upfront, proactive, end to end project design process in which privacy is the default setting. As applied here it has three main components: (a) a foundation of clearly articulated privacy principles; (b) a process (e.g. a privacy impact assessment) for assessing the privacy risks in a specific project design; and (c) an infrastructure of information security practices and privacy protection approaches, policies and procedures that mitigate those risks.

5.2 Privacy Impact Assessments

A carefully conducted privacy impact assessment or PIA (also referred to as Data Protection Impact Assessment or DPIA) ensures that a specific study design includes required protections of data subjects' personal data and privacy so that they do not experience adverse consequences or harms as a result of having participated in research. Simply stated, a PIA is a process to systematically identify and mitigate risks to data subjects' personal data and privacy over a project's life cycle. It typically involves four steps:

1. *Chart the planned flow of information through the organisation(s).*
2. *Identify potential risks, their severity and likelihood.*
3. *Develop and evaluate solutions that mitigate any identified risks.*
4. *Integrate risk mitigation solutions into organisational processes and plans.*

For a more detailed treatment consult the ESOMAR/GRBN Guideline on Duty of Care: Protecting Research Data Subjects from Harm.

5.3 Information Security Practices

The ESOMAR Data Protection Checklist provides a step-by-step evaluation process to identify gaps and develop solutions in an organisation's information security infrastructure and practices. Researchers should consult it as part of the risk mitigation phase of a PIA.

---

[1] *The Organisation for Economic Cooperation and Development (OECD) espouses a similar set of privacy principles that comprise a privacy framework reflected in many existing and emerging privacy and data protection laws worldwide. See OECD Privacy Framework for details.*

6 Sampling

The first step in sampling typically involves identification of a database from which a sample is drawn using probability or non-probability selection procedures. Examples include lists compiled from public and private sources (e.g., websites, lists of telephone numbers, magazine subscribers, professional association members, registered voters, and so on), lists of the client's customers, and online access panels constructed explicitly for research or marketing purposes.

Sample sources may also be created dynamically at the time of selection as is done increasingly in online research and even offline via techniques such as mall intercepts and snowball sampling. Often these sources contain personal data in the form of direct identifiers that can be used to contact prospective data subjects. [2]

Regardless of the type of sample, researchers must undertake the necessary steps to verify the provenance of all data sources. This is required to ensure that all personal data has been collected, processed and transferred legally within the requirements of any given jurisdiction and that there are legitimate grounds to use the data for research purposes. At a minimum, researchers must ask the following questions and receive satisfactory answers in return:

1. *How was the data source constructed and by whom?*
2. *Did the data collector obtain the consent of data subjects, for what purpose, and were data subjects made aware that they might be contacted by third parties?*
3. *How is the data source maintained and kept current?*
4. *Does the data source contain children and/or known vulnerable individuals?*
5. *For what purposes other than research is the data source used?*
6. *Are there any known problems with the data?*

For further discussion of the use of data not collected directly from data subjects but available from another source consult the forthcoming ESOMAR/GRBN Guideline When Processing Secondary Data For Research or the MRS Checklist for Buying and Using Data Lists. When procuring samples for studies to be conducted online, researchers should also consult ESOMAR's Questions to Help Buyers of Online Samples.

Finally, given that sample files typically include personal data, research organisations must provide the same level of protections they would for any data in their possession that also contains personal data, including during transfer from one organisation to another.

7 Solicitation

The approaches for contacting data subjects for research are governed by two separate traditions.
Traditional (offline) research methods (e.g., face-to-face, telephone, focus group recruitment, etc.), which by their nature, of having direct contact with individuals, makes soliciting their cooperation relatively straightforward. However, there still are a number of legal and ethical requirements that must be met. They include but are not limited to:

- *Do Not Call lists and restrictive laws and/or limits on calling hours;*
- *limitations on the use of autodialling equipment;*

[2] *One exception is online panel samples in which individual identities are protected by the sample supplier and not shared with the researcher.*

- *where autodials are permitted, limits on silent/abandoned calls and prohibitions against suppressing the identity of calling numbers; and*
- *honouring requests from data subjects to not be contacted again.*

As with all other aspects of research, researchers must respect the privacy choices of data subjects.

Solicitation for online studies is typically much more challenging due to heightened privacy concerns and the relative ease with which large numbers of data subjects can be contacted electronically. Local and national laws may vary in their treatment of email and text messages. In some countries using automated systems to send text messages is prohibited unless explicit consent is obtained. Researchers must not use any subterfuge in obtaining email addresses or mobile phone numbers of data subjects. This includes the use of public domains, the use of technologies or techniques without individuals' awareness, or collecting under the guise of some activity other than research. As technologies have evolved so have methods of directly contacting individuals to engage in research. These include various types of mobile apps and direct contact through social media.

Regardless of the technology used, researchers must not contact individual data subjects directly to solicit participation unless there is a reasonable expectation on the part of the data subject that they may be contacted for research. Such agreement can be assumed when ALL of the following conditions exist AND where there are no restrictions or prohibitions based on local laws and/or regulations:

- *A substantive pre-existing relationship exists with the entity supplying the sample such as the client, the research organisation or sample company.*
- *Where data subjects have specifically opted-in for online or mobile research with researchers or sample providers, or in the case of client-supplied lists of customers who have not opted-out of direct communications and may be contacted for research.*
- *Any invitations sent to data subjects must clearly communicate or link to the names of sample providers, researchers or clients, and their relationship with data subjects clearly offer the choice to be removed from future contact.*
- *Sample files exclude in an appropriate and timely manner all data subjects who have previously requested removal from contact.*
- *Data subjects who have not been recruited via unsolicited email, text message, or other similar avenues.*

Researchers must also note that:

- *When receiving contact information from clients or sample providers, researchers must verify that those listed have a reasonable expectation that they will receive some form of contact for research purposes.*
- *Researchers must not use false and/or misleading information when recruiting data subjects.*
- *It is good practice, and in some countries a requirement, for researchers to keep copies or records of messages and other documents received from data subjects agreeing to or restricting the access and use of their personal information.*

For further discussion of privacy protections while processing personal data in samples see Section 10 Post Processing.

8 Establishing Grounds for Collecting and Processing Data

Data protection frameworks worldwide increasingly require that individuals and organizations establish clear and compelling grounds before collecting and/or processing personal data. These requirements apply equally to researchers. Even in jurisdictions where such legal requirements do not exist, the responsibility that researchers bear to respect the privacy and rights of data subjects requires that they establish some basis for collecting and/or processing any personal data.

8.1 Choosing Specific Grounds

While the requirement to establish grounds for collecting and/or processing personal data is increasingly common worldwide there are often significant differences across jurisdictions in terms of available grounds, how to qualify, and what specific data collection and/or processing activities are permitted. Therefore, researchers must fully understand the requirements within all jurisdictions applicable to the personal data being collected and ensure that they comply with the relevant law.

One common theme across all available grounds is that the privacy, rights, and well-being of data subjects be the primary concern.

While there are a number of grounds that can be used, researchers historically have relied on data subjects' consent when engaged in primary data collection.

8.1.1 Notification, Consent, Transparency, and the Voluntary Nature of Research

The specific requirements for consent vary considerably across jurisdictions and researchers must ensure that those requirements are met in all countries where they collect or process data. At a minimum, researchers must be fully transparent about the information they plan to collect, the purpose for which it will be collected, how it will be protected, with whom it might be shared and in what form. The information must be clear, concise and readily available to data subjects, either through direct links (as in online methodologies) or by request.

In the case of online samples, this responsibility is shared by the sample provider and the researcher. While the sample provider has a responsibility to protect any personal data that it owns and controls, including setting the general rules that govern interactions with sample members, researchers must ensure that the terms set out in the above paragraph are communicated to data subjects each time they are invited to complete a survey.

Researchers must never mislead, lie, trick or coerce data subjects to participate in research. Participation in research is always voluntary and researchers must ensure that data subjects are allowed to withdraw and have their data deleted at any time.

Researchers also must clearly distinguish research from other non-research activities. In addition, researchers must not allow any personal data collected to be used for any other purpose than research unless data subjects have consented to this at the time of data collection.
If at any time during a research project there are material changes in a research plan (for example, additional passive data collection such as location or identifiable data shared with research user clients), researchers must notify data

---

[3] *Where there are genuine concerns about bias if the client is disclosed up front, researchers may choose to wait until the data subject has completed the research task before disclosing the client's name. However, this approach can only be used with the agreement of the data subject.*

subjects so that they can make an informed choice about whether to continue in the research.
In cases where research involves multiple waves of data collection or extends for several months or longer, researchers must periodically refresh consent by reminding data subjects of the data being collected, the purpose for which it is being collected, and how it is being used. Times when researchers must refresh consent include, but are not limited to, when there is a material change to data collection or data use practices; a change in a research organisation's ownership; or a change in applicable laws and regulations.

When researchers use third parties for data collection services, researchers must ensure that all data is sourced lawfully and ethically.

8.1.2 Legitimate Interest

Legitimate interest provides an alternative ground that can be used for collecting and processing personal data without requiring consent. Legitimate interest can be a suitable ground for processing where the personal data is being used for research purposes in a manner that data subjects would reasonably expect, and the processing is unlikely to have a significant impact on their rights and privacy.

When determining whether legitimate interest can be used, researchers must ensure that their interests are not being given priority over the fundamental rights and freedoms of data subjects. To that end, they must follow and document a three-stage approach addressing these criteria:

- *Purpose – is a legitimate interest being pursued?*
- *Necessity – is the collection and processing necessary to fulfill the purpose?*
- *Balancing – do the data subjects' rights and interests override the researcher's interest?*

The process of considering and weighing participant interests when considering the use of legitimate interest must be documented in some way, for example, as a Legitimate Interest Assessment. It should also be noted that in some jurisdictions legitimate interest cannot be used for processing of sensitive data (sometimes called special category data) or when the data is to be used for automated decision making.

8.1.3 Contract

Contract also can be used as a basis for processing personal data. Researchers can use this basis if they need to process a data subject's personal data in order to fulfill contractual obligations toward data subjects. While this has limited application in the research context it can be applicable for the administration and management of access panels.

8.1.4 Public Task and Interest

Processing of personal data that is necessary for the performance of a task in the public interest or for official functions is another basis that researchers may consider. The conditions for using this basis tend to be tightly defined and vary between countries. As a result, it is primarily used for public sector research and/or private sector research which clearly demonstrates public interest. It should also be noted that requirements and conditions for using this

---

[4] *There may be rare instances in which a researcher might find it necessary to mislead a data subject in order to comply with the research purpose. In all such instances, researchers must inform data subjects and correct any misinformation provided at the conclusion of the research , and data subjects must be offered the opportunity to delete their data and not be contacted again for the research. Examples include certain types of advertising testing and message testing in political polling.*

legal basis vary between countries.

9 Additional Considerations

9.1 Sensitive Data

Researchers must take appropriate steps to protect participants when approaching data subjects with topics having a sensitive nature due to legal requirements and also due to the potential risk of harm or distress for data subjects. Researchers must ensure that any sensitive data collection approaches are necessary, relevant and clear. Researchers must explain the purpose of any sensitive questions, obtain the data subject's explicit consent and ensure that data subjects have the option to "prefer not to answer" or other options that allow data subjects to not provide any sensitive information that may be being sought.

In some countries, authorisation to collect sensitive personal data may be required from the relevant national authority.

9.2 Protecting Against Harm

Researchers have a duty of care to ensure that data subjects are not harmed or adversely affected in the course of participating in a research project. This includes any type of harm e.g. financial, physical, or emotional. To that end, researchers must consider carefully the specific requirements of the research, consult local legal requirements/ restrictions and regulations, and consider practical implications that any research may have on data subjects. In particular, researchers must:

- *avoid misleading statements that would be harmful or create a nuisance to the data subject (e.g. inaccurate information about the research content, likely length of the interview or the possibility of being re-interviewed on a later occasion, via online or other interviewing techniques);*
- *avoid misleading or unsolicited data collection and processing (e.g. undisclosed automated systems that gather personal data from online environments/mobile devices) where users have an expectation of privacy and of being asked for their consent on specific actions; and*
- *respond to any inquiries data subjects may address to researchers.*

For further discussion consult the ESOMAR/GRBN Guideline on Duty of Care: Protecting Research Data Subjects from Harm.

9.3 Qualitative Research

Data subjects participating in qualitative research are entitled to the same protections as those in quantitative studies. These studies can pose a special challenge in that some forms, such as focus groups, may include participation by clients or other third parties. Examples include viewing live-streamed focus groups, viewing video recordings of focus groups or in-depth-interviews, and even direct interaction between the client and data subjects.
In all cases, researchers must ensure that in the process of gaining consent:

- *data subjects are made aware that clients or other third parties may participate, the form of that participation, in what capacity clients or third parties are participating and steps to be taken to protect any personal information disclosed during the research;*
- *clients must agree to only collect personal data that data subjects have agreed to share; and*
- *clients must agree to keep confidential any personal information about data subjects disclosed during the research.*

9.4 Children, Young People, and Other Vulnerable Individuals

There are special requirements for contacting and gaining consent when doing research with children and other vulnerable individuals. Consult the ESOMAR/GRBN Guideline on Research and Data Analytics with Children, Young People, and Other Vulnerable Individuals for details.

9.5 Passive Data Collection

Sometimes called observational research, passive data collection comes in many forms, with differing methods of data collection including audio and video recording, collection of online browsing histories, scraping of social media postings, and recording of purchasing behaviour, to name a few. Some of these methods are classified as primary data collection, i.e. collected by a researcher for a research purpose. In those instances, the researcher must follow the process described in this guideline.

However, some methods are best classified as secondary data research, i.e. the data is collected by someone else. It is the researcher's responsibility is to confirm that the data was collected legally and there are legitimate grounds to process it for a research purpose. Consult the forthcoming ESOMAR/GRBN Guideline for When Processing Secondary Data for Research for further discussion of the researcher's responsibilities when using these secondary data sources.

9.6 Mystery shopping

Researchers carrying out mystery shopping studies must take care to ensure that individual privacy is respected and data subjects (typically store personnel or similar) are not disadvantaged or harmed as a result of the study. Before undertaking a mystery shopping study, researchers must first confirm that the client has previously obtained the consent of data subjects meeting all requirements described above, that any personal data collected is fully protected and only released to clients with the consent of the data subjects.

Researchers also must take care to ensure that no personal data of any kind (including photos or recordings) is collected about individuals for whom no consent was obtained. Examples include other shoppers or store personnel in competitor stores.

For further discussion see the ESOMAR/GRBN Guideline on Duty of Care: Protecting Research Data Subjects from Harm.

9.7 Online tracking techniques

A number of technologies used for online marketing activities (e.g. cookies, tracking pixels, device IDs) have valid application in research in areas such as online audience measurement, content measurement, advertising testing and online sample management (e.g. fraud detection), to name a few.

Where possible, researchers must obtain consent based on how personal data will be collected, used, and reported. However, there may be instances in which consent is not possible and so researchers must rely on other legally permissible grounds. Legitimate interest is one such ground. Under these circumstances, researchers must remove or obscure any identifying characteristics as soon as operationally possible.

9.8 Incentives

Where incentives are offered to encourage participation, researchers must ensure that data subjects are clearly informed about:

- *who will administer the incentives;*
- *what the incentives will be;*
- *when data subjects will receive the incentives; and*
- *whether conditions are attached e.g. completion of a specific task or passing of quality control checks (for example with online panel research).*

Researchers also must ensure that incentives are proportionate, do not constitute, or are perceived to constitute,

a bribe, and comply with legal requirements for the jurisdiction in which they are offered. Incentives must be appropriate for the audience and the nature of the research. For example, if research is focused on driving habits it would be inappropriate to offer alcoholic drinks as an incentive.

The use of client-supplied incentives and/or offers of discounts, whereby data subjects would be required to spend money in order to benefit from the incentive (for example price discounts on goods and services that would require data subjects to pay the balance in order to gain any benefit) must not be offered as incentives as such activity falls within the scope of direct marketing (as the client supplied incentive and discounts are deemed to be a form of client promotion).

Researchers must ensure that data collected in order to administer incentives is not used for any other purpose, e.g. database building. They must not pass identifiable data subject details, collected as part of the incentive process, to clients (including internal clients if conducted within a client-side research department) and/or any other third party without the consent of data subjects.

Finally, when undertaking cross-border, multi-country online research projects, researchers must ensure the process for offering incentives must adhere to all relevant laws of all the countries involved.

9.9 Sweepstakes and free prize draws (also called lotteries)

These types of incentives are often tightly regulated, and researchers must be aware of all applicable local laws and rules, which vary across countries. For further discussion refer to Appendix A.

10 Post Processing

Researchers must ensure that during post processing (a) the privacy of data subjects is fully protected and (b) no errors are introduced during processing and analysis. In both cases researchers must have in place a set of procedures and standards designed to accomplish these goals.

10.1 Privacy Protection

The ESOMAR Data Protection Checklist provides a road map to an infrastructure of technologies, standards and processes designed to prevent the inadvertent disclosure or loss of personal data. Researchers should use it as an assessment tool of their privacy protection program to identify gaps and develop solutions.

A key concern is that personal data is not disclosed to clients. Unless applicable privacy laws and/or regulations stipulate a higher requirement, researchers must only communicate a data subject's personal data to a client under the following conditions:

- *the data subject has given explicit consent and*
- *the purpose is for research only.*

Further, it is essential that researchers obtain from clients a written guarantee that the client will not attempt to identify participants unless the above conditions are met. For further discussion consult the ESOMAR/GRBN Guideline on Duty of Care: Protecting Research Data Subjects from Harm.

Researchers also must ensure that any personal data shared with a subcontractor be limited to what is required to perform the subcontracting task(s) and that the subcontractor has the necessary information security procedures in place to protect the data. The subcontractor's responsibility for data protection must be clearly documented and agreed to.

10.2 Documentation

Researchers must fully document the specific post-processing steps performed including any cleaning, merging with other data sources, weighting, imputation (if used) and specific analyses undertaken. The documentation should be specific enough for a data user to understand how the data may have been altered post data collection.

Responsibilities to Clients and Other Data Users

11 Transparency

11.1 Project Design

Researchers must recognise and meet their ethical responsibilities to clients and sponsors who commission research. This requires that researchers design research to meet the objectives, specifications and quality proposed and agreed to with clients or sponsors. Researchers must be transparent about the way in which research is to be executed from beginning to end. This information typically is communicated to clients at the proposal stage, and then modified as the work progresses. The ISO standard, ISO 20252:2019 - Market, opinion and social research, including Insights and Data Analytics -- Vocabulary and service requirements, provides a detailed list of project design features that should be disclosed to clients at the proposal stage and updated as the research unfolds. Adherence to the requirements set forth should be followed to ensure full transparency of the specific data collections and analyses to be performed.

11.2 Subcontracting

Researchers must inform clients, prior to work commencing, when any part of the work is to be subcontracted outside the researcher's own organisation. On request, clients must be told the identity of any such subcontractor.

Researchers are also required to ensure that any personal data shared with a subcontractor be limited to what is required to perform the subcontracting task(s); that the subcontractor has the necessary data security procedures in place to protect the data; and that the subcontractor's responsibilities for data protection are clearly documented and agreed to.

11.3 Analysis, Reporting and Delivery

If users of research are to have confidence that delivered data is fit for purpose, then researchers must make available appropriate information to those users about how the research was conducted, including any limitations of the methodology that might lead to conclusions not supported by the data. At a minimum, this information must include:

- *the name of the organization that funded the research, the organization that conducted it, and any subcontractors used;*
- *the definition of the target population, sample source and size;*
- *sample design and selection procedure;*
- *the incentive used (if any) and how it was administered;*
- *where appropriate, a response or participation rate and how it was calculated;*
- *the method of data collection and a copy of any instruments used;*
- *any data cleaning, weighting or post-field adjustments that may have been applied; and*
- *a statement of substantive limitations affecting the validity of findings.*

Researchers should review the more comprehensive set of reporting requirements set forth in the ISO standard, ISO 20252:2019 - Market, opinion and social research, including Insights and Data Analytics -- Vocabulary and service requirements.

Responsibilities to the General Public

12 Publishing results

When a client plans to publish the results of a research project, both the client and the researcher have a responsibility to ensure that the published results are not misleading. To that end, clients should consult with the researcher on the form and content of publication of the findings.

Researchers also must be prepared to make available on request technical information sufficient to assess the validity of published findings. This includes relevant information on the background of the study, the sample source, the method of data collection, the wording of any questions used, any weighting that was employed, and any tables or other analytic outputs reported on in the publication. For further details consult the ESOMAR/WAPOR Guideline on Opinion Polls and Published Surveys

Researchers must not allow their name to be associated with the dissemination of conclusions from a research project unless those conclusions are adequately supported by the data.

13 References

ESOMAR Data Protection Checklist
ESOMAR/GRBN Guideline on Research and Data Analytics with Children, Young People, and Other Vulnerable Individuals
ESOMAR/GRBN Guideline on Duty of Care: Protecting Research Data Subjects from Harm
ESOMAR/GRBN Guideline When Processing Secondary Data for Research
ESOMAR/WAPOR Guideline on Opinion Polls and Published Surveys
ICC/ESOMAR International Code on Market, Opinion, and Social Research and Data Analytics
ISO 20252:2019 - Market, opinion and social research, including Insights and Data Analytics -- Vocabulary and service requirements
MRS Checklist for Buying and Using Data Lists
OECD Privacy Framework
Questions to Help Buyers of Online Samples

14 Project Team

Reg Baker, North American Regional Ambassador, ESOMAR
Debrah Harding, Managing Director and Finance Director, Market Research Society
Joke Ruwen-Stuursma, Professional Standards Executive, ESOMAR
Judith Passingham, Chair of the Professional Standards Committee, ESOMAR
Andrew Canon, Executive Director at GRBN

A number of individuals also provide useful comments on an earlier draft:

Pepe Aldudo, ANEIMO
Sandesh Banawaliker
Jeremy Brodsky, Gutcheck
Gerrit Burghardt, Searchlight Pharma
Evan Davies, YouGov
Jackie Lorch, Dynata
Adam Phillips, Real Research
Angela Priest, Gutcheck
Ashlin Quirk, Dynata
Fred Schipper, Ipsos
John Tabone, CRIC

15 APPENDIX A

Sweepstakes and Free Prize Draws

Sweepstakes and Free Prize Draws as a form of incentive was popular in the early days of online research, but their use has declined due to lack of effectiveness and the significant risks of using them without the necessary detailed knowledge, for example in some countries:

1. Data subjects must not be required to do anything other than agree to participate in online research projects to be eligible for entry to a free prize draw or sweepstake. This includes not having to provide responses to research questions, complete surveys, etc. which may be part of a research project, especially where a disproportionate amount of data is supplied by the individual, as this may be considered as a data subject "transferring money's worth". In such cases it would be viewed in the same way as a requirement to pay to participate and would become a paid lottery subject to statutory controls.
2. Some form of skill may be required for entry to free prize draws/sweepstakes in order for them to be classified as such e.g. asking a question which requires some knowledge, albeit relatively easy (e.g. Who is President of the US?), before entry is accepted.
3. Failure to complete research activities or projects does not disqualify data subjects from entering a free prize draw or sweepstake.
4. Researchers must not withhold free prize draw/sweepstake prizes unless data subjects have clearly not met criteria set out in the rules underpinning a free prize draw/sweepstake (e.g. rules restricting family members of staff responsible for a free prize draw or sweepstake participating in a draw).
5. Researchers must ensure that all relevant information regarding free prize draws/sweepstakes is clearly communicated to data subjects at the time consent is asked. Specific requirements vary between countries, but include information such as:

o the closing date of entry;

o the nature of the prize;

o if a cash alternative can be substituted for any prize;

o how and when winners will be notified of results;

o how and when winners and results will be announced;

o qualification and disqualification criteria; and

o alternative means of entry.

6. All rules must be clear and unambiguous so that they are easily understood by data subjects and not misleading. This includes the chances of winning, the value of prizes offered, and so forth. In addition:

o such rules must not be unreasonable and/or unduly restrictive;

o researchers must clearly distinguish between gifts offered to all or most free prize draw/sweepstake data subjects, and prizes offered to the winners;

o researchers must ensure that alternative free means of entry are available for all free prize draws/sweepstakes and that the odds of winning are equal for all forms of entry;

o researchers must ensure that winners for free prize draws/sweepstakes are selected in a manner that ensures fair application of the laws of chance. The process by which winners are selected must be supported by a clear audit trail and any draw must be independent. In some countries independent observers may be required, to ensure all data subjects have an equal chance of winning, when a draw takes place; and

o researchers must ensure that clients are made aware of their liabilities, and potential liabilities, for any free prize/ draws/sweepstakes undertaken on their behalf. Researchers should discuss with clients approaches for mitigating such liabilities (e.g. the inclusion of third party and liability indemnification provision).

Researchers must always check national association guidelines and local laws before undertaking an exercise of this kind.