Global Guideline

Online Research

ESOMAR
WORLD RESEARCH

GLOBAL RESEARCH
BUSINESS NETWORK
APRC • EFAMRO • ARIA

ESOMAR, the World Association for Social, Opinion and Market Research, is the essential organisation for encouraging, advancing and elevating market research. www.esomar.org

GRBN, the Global Research Business Network, connects 38 research associations and over 3500 research businesses on five continents. www.grbn.org

CONTENTS

1 INTRODUCTION AND SCOPE

In 2011 ESOMAR, working jointly with CASRO, released a Guideline for conducting Online Research. In 2015, the ESOMAR/GRBN Guideline on Online Sample Quality was released.Researchers are encouraged to consult the latter document as well as this Guideline when designing and conducting online surveys.

While many of the technical and methodological issues involved in online research have been clarified over the last decade, ongoing developments in technology and in the types and variety of digital data that can be collected online require ongoing review and updates to professional and ethical guidance.

This ESOMAR/GRBN Guideline for Online Research has a global focus and explains how to apply some of the fundamental principles of market, social and opinion research in the context of the current legal frameworks and regulatory environments around the world. Thus, this document is a statement of principles rather than a catalogue of existing regulations. The objective is to support researchers, especially those in small and medium-sized research organisations, in addressing legal, ethical, and practical considerations in using new technologies when conducting research online.

This Guideline is not intended to substitute for a thorough reading and understanding of the ICC/ESOMAR International Code on Market and Social Research, which has been adopted by over 60 local associations worldwide, or the individual codes of the 38 associations that comprise the GRBN. Rather, it is intended to be an interpretation of the foundational principles of those codes in the context of online research.

It also is essential that researchers review and comply with the national and local data protection and market research self-regulatory requirements of each country where they plan to collect or process data, as there may be differences in how basic principles are implemented within a specific country. The guidance provided in this document is a minimum standard and may need to be supplemented with additional measures in the context of a specific research project. Researchers may find it necessary to consult with local legal counsel in the jurisdiction where the research is to be conducted in order to ensure that they are in full compliance.

Researchers must be sensitive to consumer concerns and remain mindful that market research relies on public confidence for its success. Researchers must avoid activities and technology practices that risk undermining public confidence in market research.This includes the application of sound methodological principles and practices with respect to research design, especially in regard to appropriate questionnaire design, length, and participant burden. They also must remain diligent in maintaining the distinction between research and commercial activities such as direct marketing or targeted advertising. Where researchers are involved with activities that use research techniques but are not intended solely for research purposes, they must not describe those activities as market, social or opinion research.

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.

2 DEFINITIONS

Active agent technologies means technologies that capture research participant's behaviour in the background, typically running concurrently with other activities. They include:

- Tracking software that can capture the research participant's actual online behaviour such as web pages visited; online transactions completed; online forms completed; advertising click-through rates or impressions; online purchases; and GPS information for a computing device with an Internet connection. This software also has the ability to capture information from the research participant's email and other documents stored on a device such as a hard disk. Some of this technology has been labeled "spyware", especially if the download or installation or datacollection occurs without the participant's full knowledge and opt-in consent.

- Software downloaded to a user's computing device (computer, tablet, smartphone, etc.) that is used solely for the purpose of alerting potential survey research participants about survey opportunities, downloading survey content or asking survey questions. It does not track research participants as they browse the Internet and all data collected are provided directly from user input.

Active research means the collection of data through direct interaction with the research participant (e.g. a survey, a focus group, or other research methodology, either in-person or via some other means of communication, such as telephone, mail, or online, including email, text message or other electronic means).

Business-to-business research (B2B) means the collection of data from or about legal entities such as businesses, schools, non-profits, and so forth.

Business-to-consumer research (B2C) means the collection of data from or about individuals or households.

Cloud computing means deploying groups of remote servers and computer networks that allow centralised data storage and online access to computer services or resources. Cloud computing includes three general deployment models: public, private, or hybrid.

Commercial activity means any activity with a purpose that is not research including direct marketing and targeted advertising.

Consent means the freely given and informed agreement by a person to the collection and processing of his/her personal data.

Cookies are text files containing small amounts of information, which are downloaded to a user's device when he or she visits a website. Cookies are read or sent back to the originating website on each subsequent visit, or to another website that recognises that cookie.

Cookies are useful because they allow a website to recognise a user's device, thereby personalising the user's experience. This includes things like the ability to remember user preferences and generally making website navigation more efficient. Researchers may use cookies for several purposes including, without limitation, to provide a better survey experience, quality control, validation, to enable or facilitate survey participation, tracking of completed surveys or other completed actions, and for fraud detection and/or prevention. Cookies can be rejected or deleted through browser settings.

Data controller means a person or organisation responsible for determining how personal data are processed. For example, a research client would be the controller of data from its clients or customers; a research panel provider would be the data controller for data collected from its online panel members; and a research company would be the data controller for data collected from participants in an omnibus survey.

Data processor means a party who obtains, records, holds, or performs operations (including analysis) on personal data on behalf of and under direction of the data controller. As noted above, a research company would be both data controller and processor for an omnibus study**.**

Device ID (device identification) is a distinctive number associated with a smartphone or similar handheld device. Such a device typically will have multiple device IDs, each used for a different purpose. Some device IDs are used to enable services such as Wi-Fi or Bluetooth, or to uniquely identify specific devices operating on a mobile carrier network. Other device IDs, such as Apple's UDID or Android's Android ID, are used by apps, developers, and other companies to identify, track, and analyse devices and their users across various mobile services.

Digital fingerprint (also known as device fingerprint, machine fingerprint or browser fingerprint) is information collected about a computing device (computer, tablet, smartphone, etc.) for the purpose of identification. Digital fingerprints can be used to fully or partially identify individual research participants or devices even when cookies are disabled. They typically use web browser configuration information along with other computing device parameters that can be obtained. This information is assimilated into a single string that comprises the digital fingerprint.Digital fingerprints are also used in non-research applications and have proven useful in the detection of online identity theft and credit card fraud prevention.

In some jurisdictions, digital fingerprints may be considered personal data and must be treated as such, including the need for consent.

It is important to note that as the components of a digital fingerprint can change over time, the digital fingerprint associated with a device can vary as well.

In market research the term device ID is sometimes used instead of digital fingerprint. However, device ID has a different meaning (see device ID).

Free prize draw or sweepstake means a contest or drawing where prizes are allocated by chance and participants are not required to pay or undertake any activity other than to enterto have the opportunity to win. Whilst these are sometimes called lotteries, in many jurisdictions a lottery is a very specific legal term and is often prohibited for private entities such as research agencies.

Geolocation means the identification of the real-world geographic location of an object, such as a computing device (computer, tablet, smartphone, etc.). Geolocation may refer to the practice of assessing the location, or to the actual assessed location.

Incentive means any benefit offered to a participant to encourage participation in research.

Laws protecting privacy means national and local laws or regulations, the enforcement of which has the effect of protecting personal data consistent with the principles set forth in this document**.**

Local shared objects (LSOs), commonly called Flash cookies (due to their similarities with HTTP cookies), are pieces of data that websites using Adobe Flash may store on a user's device or computer.

Market research, which includes social and opinion research, means the systematic gathering and interpretation of information about individuals or organisations using the statistical and analytical methods and techniques of the applied social and behaviouralsciences to gain insight or support decision making.

Online researchmeans the use of computer networks, primarily the Internet, to assist in any phase of the market research process including development of the problem, research design, data collection, or analysis.

Paradatameans data about the process by which survey data were collected. Examples include the date and time the survey was completed; how long the survey took; and participant movement in the survey.

Passive research means the collection of data by observing, measuring, or recording a participant's actions or behaviour.

Personal data (sometimes referred to as personally-identifiable information or PII) means any information relating to an identified or identifiable natural person. An identifiable person is someone who can be identified directly or indirectly, in particular by reference to an identification number or the person's physical, physiological, mental, economic, cultural or social characteristics. In some types of research such data records could include situations where individuals might be identifiable because of photographs, video and audio recordings, or other personal data collected during the research.

PII means personally-identifiable information (or personally identifiable data). See personal data.

Private cloud means a cloud computing arrangement in which dedicated equipment in a particular data centre is assigned to the researcher's firm.

Public cloud means a cloud computing arrangement in which a service provider makes resources, such as applications and storage, available to the general public over the Internet.

Research participant means anyone whose personal data are collected for research purposes, whether by an active or by passive means.

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

Sensitive data means any information about an identifiable individual's racial or ethnic origin, health or sex life, criminal record, political opinions, religious or philosophical beliefs or trade union membership. There may be additional information defined as sensitive in different jurisdictions. In the U.S., for example, personal health-related information, income or other financial information, financial identifiers and government-issued or financial identity documents are also regarded as sensitive.

Social media research means research in which social media data are utilised either alone or in conjunction with data from other sources.

Spyware means software that asserts control over a computer or collects information about a person or organisation, without the user's knowledge, and that may send such information to another entity without the user's consent.

Subcontracting means passing responsibility for executing a portion of the research project to a third party organisation or individual, including outsourcing and off-shoring.

Tracking pixels are objects that are embedded in a web page or email and are unobtrusive (usually invisible) to the user. Tracking pixels allow the operator of a web page or the sender of an email to determine whether a user has viewed the page or email. Common uses are email tracking and page tagging for web analytics. Alternative names include web beacon, tracking bug, tag, page tag or web bug.

Transfer in relation to data refers to any disclosure, communication, copying or movement of data from one party to another regardless of the medium, including but not limited to movement across a network, physical transfers, transfers from one media or device to another, or by remote access to the data.

Transborder transfers of personal data means the movement of personal data across national borders by any means, including access of data from outside the country where collected. This can include the use of cloud technologies for data collection and storage**.**

3 PARTICIPANTS: RELATIONSHIPS AND RESPONSIBILITIES

3.1 Distinguishing market, social and opinion research from other data collection activities

Researchers must ensure that research purposes are clearly distinguished from other non-research online activities. In addition, they must not allow any personal data they collect to be used for any other purpose than market research. To clearly communicate this distinction to research participants, the researcher must present the research services and the organisation or company carrying them out in such a way that they are clearly differentiated from any non-research activities.

This requirement does not prevent researchers from being involved in non-research activities, providing the purpose of collecting any personal data is not misrepresented and that any personal data are not used for another purpose unless specific informed consent is obtained from each participant. Nor do they in any way restrict the right of the organisation to promote the fact that it carries out both market research and other activities providing they are clearly differentiated and that they are conducted separately and in accordance with the relevant laws, regulations and local professional rules of conduct.

3.2 Notification, honesty, consent and the voluntary nature of research

Researchers must obtain informed consent from research participants before collecting and processing any form of personal data and be completely 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 should be clear, concise and prominent. This includes, but is not limited to, the use of best practices inprivacy policies, the prominent placement of links to privacy policies in questionnaires and panel sites, and communication

throughout the data collection and data use processes. Participants must never be misled, lied to, tricked or coerced. Participation in research is always voluntary and participants must be allowed to withdraw and have their personal data deleted at any time.

This Guideline also recognises that in some situations obtaining consent may not be possible. See 3.2.1 for further discussion.

If at any time during the research there are material changes in the research plan (for example, additional passive data collection such as location or identifiable data shared with research user clients), participants must be informed so that they can make an informed choice about whether to continue in the research. In the case of an access panel or research community or when research involves multiple waves of data collection or extends for several months or longer, researchers should periodically refresh consent by reminding participants of the data being collected, the reasons for collecting the data and the intended use.The times when consent should be refreshed include, but are not limited to, when there is a material change to data collection or data use practices; a change in the research organization or ownership; or a change in applicable laws and regulations.

Finally, researchers must comply with all relevant laws, regulations and local professional rules of conduct.

3.2.1 Passive data

New technologies now make it possible to collect a broad range of personal data without direct interaction with the individuals whose data are collected.

Examples include, but are not limited to, web browsing data, loyalty cards and store scanners, geo-location data from connected devices, and some types of social media data. As mobile technology continues to evolve, many of these data sources also can be accessed from and via mobile devices.

In situations where researchers collect cross-site browsing data from panel members or from mobile applications, a detailed description about the specific data being collected and the method(s) used to collect them must be provided to the participant and explicit consent must be obtained before such data are collected. This is particularly the case for those mobile apps that engage in geo-location, passive listening, and/or metering of the mobile devices operating system.

Where personal data are collected from public spaces such as websites or social media sites, consent must be obtained directly or explicitly provided for in the Terms of Use (ToU) policy of the platform. This does not apply to publication in social media that includes the author’s name, which implies a diminished expectation of privacy.

Some associations, including CASRO and ESOMAR, have guidelines specific to social media and they should be consulted for more detail. A combined ESOMAR/GRBN Guideline on Social Media is currently in development with the expectation of release in early 2016.

Where researchers use third parties for data collection services, the onus is on the researcher to ensure that the data have been sourced lawfully.

As there may be differences in how regulations are implemented in each country,[1]researchers must review and comply with the national and international data protection regulations and market research self-regulatory requirements of each country where they plan to collect or process data.

If researchers pass on comments to a third party without consent, they must ensure that they report only depersonalised data using techniques such as masking the comments.

In conducting all research projects, research companies must provide a clear and accessible privacy policy on their data collection and privacy practices including how to contact the research company.

Furthermore, the researcher is obliged to protect the privacy and security of any personal data regardless of how it was obtained. This includes the research organisation anonymising data before sharing it with third parties, and having a contract with the recipient of the data in which the latter agrees to make no attempt to re-identify individuals or to use such data for a non-research purpose.

3.2.2 Sensitive data

Although the online methodology is a less intrusive data collection mode than others, and allows researchers to broach sensitive topics more easily than with face-to-face or telephone interviews (with the presence of an interviewer), researchers nonetheless must be careful when approaching participants with topics having a sensitive nature either due to legal requirements or due to the risk of harm or distress the participant.

Researchers must ensure they explain the purpose of the survey sensitive questions, obtain participant's explicit consent, mention that data processing is anonymous and confidential, each question has a "prefer not to answer" option, or other option that allows the participant to not answer any sensitive question they do not wish to answer, and ensure that the questions are necessary, relevant and clear. If these protections cannot be provided because of the research design, the participant must be made aware and provide his/her explicit consent.

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

3.3 Ensuring no harm

Researchers must take all reasonable precautions to ensure that online research participants are not harmed or adversely affected by participating in a research project. This includes any type of harm e.g. financial, physical, or emotional. To that end, they should consider carefully the specific requirements of the research, consult local legal requirements/restrictions and regulations, and consider practical implications that the survey may have on participants. Inall cases, researchers must apply fair treatment principles. These include:

- avoiding misleading statements that would be harmful or create a nuisance to the participant(e.g. inaccurate information about the research content, likely length of the

[1]Consent is required in many jurisdictions to collect, process and share personal data. Some jurisdictions may allow exceptions for research purposes where securing consent is demonstrably unfeasible and if the analysis provided to the client is in the form of de-identified data.

interview or the possibility of being re-interviewed on a later occasion, via online or other interviewing techniques);

- avoiding 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

- responding to any inquiries participants may address to the market research agency/researcher.

The researcher must ensure that personal data cannot be traced nor an individual's identity inferred via cross-analysis (deductive disclosure), small samples, or in any other way through research results. Examples include merging in of auxiliary information such as geographic area data or the ability to identify a specific research participant.

3.4 Data protection and privacy

Researchers must adhere to universal data protection principles for personal data. These principles state that any personal information collected and held must be:

- collected for specified research purposes and not used in any manner incompatible with these purposes;

- adequate, relevant and not excessive in relation to the purpose of the research for which they are collected and/or further processed;

- stored separately from the response data if possible; and

- preserved no longer than is required for the purpose for which the information was collected or further processed.

Researchers must also comply with all applicable national and local laws and regulations.

3.4.1 Privacy policies

Privacy laws and regulations all typically require that research companies post a privacy policy on their website. These privacy policies must inform research participants what personal information are collected, how they are used, how they will be managed (stored and accessed), shared, and the conditions under which they may be disclosed to a third party. Privacy policies also must describe how to obtain more information or lodge a complaint. They must also be made available (typically as a link) in all online research and on relevant websites and electronic communications.

Participants must also be informed of the law(s) under which the data are being collected. If collecting data in several countries, the researcher must comply with the laws of the countries in which research is taking place. Where it is possible to know the participants' country of residence, researchers must follow the legal requirements of that country noting that there can be considerable variation across jurisdictions.

3.4.2 Data security

Researchers must ensure that security protocols are in place that protect against risks such as loss, unauthorised access, destruction, use, modification, and disclosure. Accordingly, researchers must deploy rigorous data security measures.

There are various standards and frameworks for researchers to use in developing the necessary data security standards and policies. For more information researchers can consult ISO 27001: Information technology - Security techniques - Information security management systems - Requirements or the ESOMAR Data Protection Checklist.

3.4.3 Breach notification

Researchers must comply with all relevant laws and regulations with respect to breach notificationand protocol requirements.In the absence of such applicable laws and regulation, researchers must report security or data breaches to all affected parties including clients, research participants and subcontractors without unreasonable delay. The notice should include a description of the types of data that were involved in the breach and any steps individuals should take to protectthemselves from potential harm resulting from the breach.

3.4.4 Transborder transfers

Before personal data are transferred from the country of collection to another country, the researcher must ensure that the data transfer is legal, and that all reasonable steps are taken to ensure the privacy and security of those data. This applies if a data collection server is located in a different country. Thisprinciple will also apply if cloud technology is used and the cloud servers are located in a different country (see section 7.7).

3.5 Email and text solicitation

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.[2] Researchers must not use any subterfuge in obtaining email addresses or mobile phone numbers of potential participants. 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.

Researchers must not use unsolicited emails or text messagesto recruit research participants or engage in surreptitious data collection. Here “unsolicited” means that participants have not granted consent or donot have a reasonable expectation that they may receive such emails or text messages.

Individuals contacted for research by email or SMS text message must have a reasonable expectation that they may receive email or text message contact for research. Such agreement can be assumed when ALL of the following conditions exist AND there are no restrictions or prohibitions based on local laws and/or regulations:

[2]Again, laws and/orregulations regarding the use of automated systems for telephone dialing and text messaging of mobile phones vary by jurisdiction. In some jurisdictions there are exceptions for research purposes whereas in some, consent is required. One specific jurisdiction worth noting is the United States where the Telephone Consumer Protection Act (TCPA) requires consent to contact a mobile phone with automated systems for telephone dialing and text messaging.

- A substantive pre-existing relationship exists between the individuals contacted and the researcher, the client supplying email addresses or mobile phone numbers, or the sample providers supplying the email addresses or mobile phone numbers (the latter being so identified or linked to by the email invitation or text message).

- Where email or text message invitees have specifically opted-in for online or mobile research with the researcher or sample provider, or in the case of client-supplied lists of customers whohave not opted-out of email or text message communications and may be contacted for research.

- Email or text message invitations to potential research participants clearly communicate or link to the name of the sample provider, researcher or client, and their relationship with the individual and clearly offer the choice to be removed from future email or text message contact.

- The email sample or mobile phone number list excludes in an appropriate and timely manner all individuals who have previously requested removal from future email or text message contact.

- Participants in the email or mobile phone sample were not recruited via unsolicited email or text message invitations.

Researchers must also note that:

- When receiving email lists or mobile telephone lists from clients or sample providers, researchers must verify with the client or sample provider that individuals listed have a reasonable expectation that they will receive an email contact or text message.

- Researchers must not use false or misleading return email addresses or any other false and misleading information when recruiting participants.

- Researchers must offer participants the opportunity to opt-out of any research project. This also applies if a participant requests to be deleted from the sample source list for blind studies (i.e. where the sponsor of the study is not cited or linked to in the email solicitation or text message but disclosure is offered to the participant during or after the interview).

- Researchers must comply with any applicable requirements of this section when using other messaging technologies such as mobile application (mobile app) for notifications that have characteristics and capabilities that are similar to text messages.

It is good practice for researchers to keep copies or records of emails and other documents received from research participants agreeing to or restricting the access and use of their personal information.[3]

3.6 Incentives

The rules for sweepstakes and free prize draws should be read in conjunction with the following rules for incentives.

[3]This is a legal requirement in some countries, including all EU (European Union) member states, Argentina, Australia, Canada, New Zealand, and U.S. (for researchers that participate in the U.S.-EU Safe Harbor program)

Where incentives are offered to encourage participation in online research projects, researchers must ensure that participants are clearly informed about:

- who will administer the incentives;
- what the incentives will be;
- when participants 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 and do not constitute, or are perceived to constitute, a bribe. Incentives must be appropriate for the audience and the nature of the research. For example, if online research is focused on driving habits it would be inappropriate to offer alcoholic drinks as an incentive.

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 participant 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 express permission of participants.

Researchers must be aware of local laws and rules regarding incentives, for example in some countries:

- The use of client-supplied incentives and/or offers of discounts, whereby participants would be required to spend money in order to benefit from the incentive (for example price discounts on goods and services that would require participants to pay the balance in order to gain any benefit) are prohibited for online research projects 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).
- Incentives must be of a specific nature (e.g. non-monetary).

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

3.6.1 Sweepstakes and free prize draws (also called lotteries)

Sweepstakes and free prize draws are an especially popular form of incentive in online research. When using them, researchers must be aware of the applicable local laws and rules, which vary between countries, and the significant risks of using this approach without the necessary detailed knowledge, for example in some countries:

- Participants 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 participant “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.

- 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.

- Failure to complete research activities or projects does not disqualify participants from entering a free prize draw or sweepstake.

Researchers must not withhold free prize draw/sweepstake prizes unless participants 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.)

Researchers must ensure that all relevant information regarding free prize draws/sweepstakes is clearly communicated to participants at the time consent is asked. Specific requirements vary between countries, but include information such as:

- the closing date of entry;

- the nature of the prize;

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

- how and when winners will be notified of results;

- how and when winners and results will be announced;

- qualification and disqualification criteria; and

- alternative means of entry.

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

- Such rules must not be unreasonable and/or unduly restrictive.

- Researchers must clearly distinguish between gifts offered to all or most free prize draw/sweepstake participants, and prizes offered to the winners.

- 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.

- 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 participants have an equal chance of winning, when a draw takes place.

- Finally, 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 before undertaking an exercise of this kind.

4 CLIENTS: RELATIONSHIPS AND RESPONSIBILITIES

4.1 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.

In cases where the identity of a subcontractor used for sample sourcing can be legitimately be considered proprietary information, the sample provider must provide:

- a description of the type of sample sources to be used; and
- an estimate of the percent of the sample expected from panel sources and non-panel sources.

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.

4.2 Protecting personal data

Researchers must ensure that research participants' personal identity is not disclosed to clients. Unless applicable privacy laws and/or regulations stipulate a higher requirement, the researcher may communicate the research participant's identifiable personal information to the client only under the following conditions:

- the research participant has given explicit consent;
- the purpose is for research only; and
- nomarketing or sales activity will be directed at the participant as a direct result of their having provided this information.

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.

4.3 Transparency, misrepresentation and correction of errors

All research projects must be reported on and documented accurately, transparently and objectively. In the event that errors are discovered after delivery, the client must be notified immediately and corrections made promptly.

For further details on reporting requirements refer to Section 6 - Methodological Quality later in this document.

5 THE GENERAL PUBLIC: RELATIONSHIPS AND RESPONSIBILITIES

5.1Maintaining public confidence

Researchers are required to verify thatsamples provided by sample suppliers or clients contain only individuals who have a reasonable expectation that they will receive email or text messagessoliciting their participation in research. Other messaging technologies such as mobile application (mobile app) notifications can have characteristics and capabilities that are similar to text messages. See Section 3.5 for further discussion.

5.2 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 are strongly encouraged to 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.

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

6 METHODOLOGICAL QUALITY

If users of online research are to have confidence that the resulting data are 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. This information should include:

- sample size, source, and management;
- sample design and selection;
- the method of data collection;
- any data cleaning, weighting or post-field adjustments that may have been applied; and
- when doing online research in countries with low Internet penetration, steps taken to ensure that the research results represent the target population of the study.

What follows is a minimum set of requirements. For further information consult theESOMAR/GRBN Guideline on Online Sample Quality.

6.1 Sample source and management

The primary categories of online sample sourcing are:

- online panels: a sample provider has developed a panel or panels from which a sample is generated;
- river or dynamically generated sample: from a traffic source on the internet;
- lists samples: such as customer lists, members of a professional association, students of a particular school, etc.

In each case, the sample provider must be prepared to make available to the researcher details of how the sample was recruited and a description of the sampling frame and how well the sample covers the target population it is meant to represent. (For example, if the sample is "NatRep" the precise definition of "NatRep" used for the sample, and which demographic, geographic or other groups are likely to be under-represented in the sample must be provided.) In addition, researchers should report completion and breakoff rates, as well as response rates where appropriate (e.g. in case of list samples) to make it possible to assess potential nonresponse bias.

The sample provider also must be prepared to make available information about procedures used to ensure the quality of the answers given and the data collected. Thisincludes:

- steps taken to validate sample sources;
- the procedures used to "on-board" prospective participants to panels, communities or lists;
- cleaning and updating procedures;
- anymonitoring of individual survey-taking performance or quality controls to minimise satisficing or fraud and the steps taken if such behaviour is identified;
- participant support procedures;
- how rewards were administered;
- whether and how new sources were integrated into the sampling frame;
- and any procedures in place to maximise sample consistency for tracking projects.

6.2 Sample selection and design

To ensure that completed interviews represent the target population and the objectives of the research design, the researcher must document any quotas or targeting selects used in sample selection, including sample source blending,the use of sample routing technology, and the incentives offered to participants.

6.3Data collection

Researchers also must share appropriate information with the research user about how the data were collected. If a questionnaire was used this information should include:

- the median or average questionnaire length;
- the wording of all questions and any filters or respondent instructions;
- the start and stop dates of data collection;
- whether the questionnaire was designed to accommodate participants using smartphones or tablets, and if not, whether these individuals were excluded from the sample, or participated in a survey not optimised for their device; and
- any need to perform special tasks such as downloading software or sharing sensitive information or personal data.

6.4Data cleaning and weighting

The researcher must document how the data were cleaned; whether completed interviews were removed from the data and why, and information about weighting or other adjustments. If imputation is used, it needs to be clear which variables have been imputed, to what extent, and the imputation methods used.

7 ADDITIONAL GUIDANCE

7.1 Collecting data from children

Collecting data from children requires permission from the child's parent or legal guardian. National rules setting the age at which obtaining such permission is not required vary substantially. Researchers must consult national laws and self-regulatory codes in the jurisdictions where the data will be collected to determine when parental permission is required or where cultural sensitivities require particular treatment.

When first contacting a potential participant whom one might reasonably expect to be a child, researchers must ask for the person's age before any other personal data. If the age given is below the nationally agreed upon definition of a child, the child must not be invited to provide further personal data until the appropriate permission has been obtained. The researcher may ask the child to provide their parent's or legal guardian's contact details so that permission can be sought.

When seeking permission, the researcher must provide sufficient information about the nature of the research project to enable the parent or legal guardian to make an informed decision about the child's participation. This includes:

- the name and contact details of the researcher/organisation conducting the research;
- the nature of the data to be collected from the child;

- an explanation of how the data will be used;
- an explanation of the reasons the child has been asked to participate and the likely benefits or potential impacts;
- a description of the procedure for giving and verifying consent; and
- a request for a parent's or responsible adult's contact address or phone number for verification of consent.

The researcher also should record the identity of the responsible adult and his or her relationship to the child.

Parents should be advised to maintain the confidentiality of their child's identity during his/her participation to the survey after he/she consents to participate to the survey, and if needed, to be ready to assist and help him/her in completing the survey as required.

Special care must be taken regarding the research topic (including important elements such as sensitive topics that might trouble the young participant or the parents) and research questionnaire design (adapted to the child's specific characteristics - age, level of understanding; informing/mentioning for both the parent/responsible adult and the child that it is not mandatory to answer to certain questions etc.)

Prior permission from the parent or responsible adultis not required to:

- collect a child's or parent's email address solely to provide notice of data collection and request permission; or
- collect a child's age for screening and exclusion purposes. If this screening leads to the decision that a child does qualify for interview, permission must then be obtained from the parent or responsible adultto continue with the interview.

7.2 Online identification and tracking technologies

A number of technologies used for online marketing activities such as online tracking have valid application in research. The use of these technologies for research is a form of passive data collection that typically includes:

- improving the integrity of online samples;
- fraud prevention; or
- research applications, including, but not limited to, online audience measurement, content measurement and advertising testing.In these and similar cases, participant consent is required.

7.2.1 Specific technologies and requirements for use in research

These include:

- cookies;

- local shared objects (also referred to as Flash cookies);
- tracking pixels; and
- digital fingerprinting and device ID.

As some of these technologies are also used for marketing activities such as online behavioural targeting, their use has led to scrutiny from legislators, regulators and privacy groups who are concerned about the potential for the monitoring of individuals' online activity without their knowledge.

Whenever possible, consent that addresses how personal data will be collected, used, and reported must be obtained. This is of particular importance when the researcher asks a research participant to download software to his or her device.Active agents can only be used with the explicit consent of the participant.

Unless direct consent or other existing agreement (such as a Terms of Use) permits otherwise:

- data must only be reported or shared in aggregate form and there must be a contract with the recipient of the data in which the latter agrees to make no attempt to re-identify individuals (see 4.2);
- personal data must never be shared with any third party (including clients); and
- data must be anonymised when it is no longer needed, if anonymisation is not possible, data must be secured using accepted best practices.

When online tracking and identification technologies are used for research they must only be used for research purposes and the overriding principles of market research must apply (see Section 3.1 for further discussion). Furthermore, researchers must comply with all relevant laws, regulations and local professional rules of conduct.

7.3 Mobile research

In general, mobile market research is considered a method that is distinct from online as covered in this guideline. Both ESOMAR and GRBN have released guidelines specific to mobile.

However, a substantial proportion of participants contacted for online research are choosing to respond using a mobile device such as a smartphone or tablet. As a consequence, researchers should consider the limitations of smartphones (e.g. screen size and download speeds) when designing online surveys.

7.4 Social media research

The evolution of social media in recent years has changed the way that hundreds of millions of people share information about themselves around the world. The concept of consumers generating their own content on the Internet has become ubiquitous. This has created new opportunities for researchers to observe, interact and gather information. Already many techniques have been developed to leverage social media such as community panels, market research online communities, crowd-sourcing, co-creation, netnography, blog mining and web

scraping. Moreover, it is likely that many more will evolve in the future as the Internet continues to evolve.

Researchers must observe the same fundamental ethical and professional principles that govern face-to-face, mail and telephone research.

Social media data often include personally identifiable information. Many regulations in this area were developed before it was possible for one person to communicate with many on publicly accessible online platforms. Updates in privacy and data protection laws are still being developed and often lag changes in practices that have become generally accepted.

Nonetheless, researchers must consult whatever local regulations or industry codes that might exist in jurisdictions where research is planned.For additional information consult section 3.2.1.

7.5 New forms of personal data

Researchers must recognise that photographs, audio, and video recordings are personal data and must be handled as such. In cases where a digital image contains an individual's face that is clearly visible so as to permit the individual to be identified, that image is considered personal data. Accordingly, all photographs, video and audio recordings gathered, processed and stored as part of a research project must be handled as personal data and protected accordingly. They can only be shared with a client or research user if the participant gives his or her consent, and then only to achieve a research purpose. Information that has been suitably anonymised (such as through pixelisation or voice modification technology) so that it is no longer personally identifiable can be shared with a client or research user client.

Consult the ESOMAR Data Protection Checklistfor additional information.

7.6Business-to-business research

A substantial number of research projects involve collection of data from legal entities such as businesses, schools, non-profits. Such research often involves the collection of information about the entity such as revenue, number of employees, sector, location, and so forth.

In all of these instances, the participating organisations are entitled to the same level of protections from identity disclosure in reporting, as those afforded individual persons in other forms of research.

It is worth noting that many national data protection laws regard an individual's title and workplace contact information as personal data. Some data protection laws go further by applying their requirements to natural and legal persons (e.g. individual people and legal entities). However legal entities have no legal access right to their data, such as research participants.

7.7 Cloud storage

The decision to store personal data in the cloud should be considered carefully. Researchers must assess the cloud storage service provider's security controls and its standard terms and conditions, and be prepared to implement compensating controls when the provider's controls are not sufficient. For example, researchers should encrypt personal data while in motion (transferred to/from the cloud) and at rest (stored on the cloud provider's servers).

Researchers also must consider the physical locations at which personal data are stored to determine whether use of cloud storage is a trans-border transfer. If personal data are to be transferred from one jurisdiction to another, it must be done in such a way that it meets the data protection requirements in both the origin and destination jurisdictions. The researcher must therefore review and understand all the applicable national and local laws and regulations to decide on the appropriate arrangements.

Researchers should seriously consider whether to locate personal data in a private cloud, rather than a public cloud. With a private cloud, dedicated equipment is assigned to the researcher's firm and the researcher always knows where the personal data are located.

By contrast, a public cloud may result in data being located in two or more data centres or two or more countries or continents, thereby raising possible compliance issues, both with applicable requirements under data protection laws and with contracts that are entered into with data controllers which specify where personal data must be located (seeESOMAR Data Protection Checklist for more details).

Finally, researchers may also want to consider purchasing a cyber-liability insurance policy. Many cloud storage service providers offer weak indemnities in the event that they cause security breaches and personal data are compromised. This means that the researcher's firm would be taking on considerable risk of financial damages and losses arising from serious privacy breaches that result in harm to the affected individuals.

7.8 Anonymisation and pseudonymisation

A key part of a researcher's data protection responsibility is to de-identify data prior to release to a client or even the general public. Anonymisation is one safeguard that involves either the deletion ormodification of personal identifiers to render data into a form that does not identify individuals. Examples include blurring images to disguise faces or reporting results as aggregated statistics so it is no longer possible to identify a particular individual.

Pseudonymisation involves modifying personal data in such a way that it is still possible to distinguish individuals in a dataset, for instance by using a unique identifier such as an ID number, or hashing algorithms whilst holding their personal data separately for checking purposes.

When employing such techniques, researchers should consult local national laws and self-regulatory codes to determine which elements must be removed to meet the anonymisation/pseudonymisation legal standard for such data.

7.9 Use of static and dynamic IDs

Historically the use of static research participant identifiers (static IDs) has been employed among research clients and sample providers to aid in the control and allocation of research participants within specific studies both longitudinal and ad hoc. This technique has helped to consolidate information about each participant and become a useful approach to ensuring unique participants within a single longitudinal study and adherence to research study exclusion

periods. In addition to improving quality control-oversee exclusion periods and sample selection, and being able to accurately identify individual research participants for studies, some researchers also require the use of static IDs to facilitate their data analysis.

Use of dynamic IDs (variable IDs for every use) have been promoted by some sample suppliers as a means to help safeguard the identity of their individual members, preventing or reducing the possibility of unscrupulous clients from utilising research participant data with other data collected (paradata) during the participants' interview session for additional insight or trying to reveal the participant's actual identity.

Researchers should carefully consider the use of each type of ID and the balancing of privacy and research quality concerns for their specific study. Legal and contractual provisions should be applied to control the collection and use of the information generated by the study within the contractual limits set up by the agreements between all parties (research participant, sample supplier, researcher, end-client).

7.10 Use and controls on paradata

It is recommended that the use of paradatais subject to mutual legal agreement between sample supplier and client to guide, limit, and protect the collection, use, and onward transfer of these data in the subsequent research process.

7.11 Unacceptable practices

Following is a list of unacceptable practices that researchers must strictly forbid or prevent. Researchers are considered to be using spyware if they use any of the following practices:

- downloading software without obtaining the participant's consent;
- downloading software without providing full, clear, concise and conspicuous notice and disclosure about the types of information that will be collected, and how this information may be used.
- using keystroke loggers without obtaining the participant's opt-in consent;
- installing software that modifies the participant's computer settings beyond that which is necessary to conduct research;
- installing software that turns off anti-spyware, anti-virus, or anti-spam software or seizes control or hijacks the participant's computer or device;
- failing to make all reasonable efforts to ensure that the software does not cause any conflicts with major operating systems and does not cause other installed software to behave erratically or in unexpected ways;
- installing software that is hidden within other software that may be downloaded or that is difficult to uninstall; or that delivers advertising content, with the exception of software for the purpose of advertising testing;
- installing upgrades to software without notifying users and giving the participant the opportunity to opt out;

- changing the nature of the identification and tracking technologies without notifying the user;
- failing to notify the user of privacy practice changes relating to upgrades to the software;
- tracking the content of the participant's email;
- if the participant's browser is set to private mode, tracking behaviour without opt-in consent; and
- when the participant is on a site, which is set to secure linkage (i.e. SSL site), collecting personal data without opt-in consent.

8 REFERENCES

- ESOMAR Data Protection Checklist
- ESOMAR/GRBN Guideline on Online Sample Quality
- Global Research Business Network
- ICC/ESOMAR International Code on Market and Social Research
- ISO 20252:2012 – Market, opinion, and social research
- ISO 26362:2009 – Access panels in market, opinion, and social research
- ISO 27001 -- Information technology - Security techniques - Information security management systems

9 THE PROJECT TEAM

- Reg Baker, Co-Chair, Consultant to the ESOMAR Professional Standards Committee, MarketingResearch Institute International
- Peter Milla, Co-Chair, Technical Consultant to CASRO, Peter Milla Consulting
- Mario Callegaro, Senior Survey Research Scientist, Google
- Melanie Courtright, Executive Vice-President - Global Client Services, Research Now
- Brian Fine, Chairman, Quality Online Research
- PhillipeGuilbert, Director General, Toluna
- Debrah Harding, Managing Director, Market Research Society

- Kathy Joe, Director International Standards & Government Affairs, ESOMAR
- Jackie Lorch, Vice President - Global Knowledge Management, SSI
- Bruno Paro, Managing Director, Netquest
- Efrain Ribeiro, Chief Research Officer, Lightspeed Research
- AlinaSerbanica, Senior Vice-President - Interactive Services, Ipsos