ESOMAR
WORLD RESEARCH

ESOMAR GUIDELINE FOR ONLINE RESEARCH

All ESOMAR world research codes and guidelines,
including latest updates, are available online at www.esomar.org

ESOMAR GUIDELINE FOR ONLINE RESEARCH

This Guideline will be updated regularly as required. It is also available as a web document with active links to other ESOMAR guidelines and useful sources. To view this guideline online go to the Knowledge and Standards, codes and guidelines section of our website www.esomar.org.

CONTENTS

1. INTRODUCTION

The ICC/ESOMAR International Code on Market and Social Research is technology neutral and applies as fully to online research as to any other form of data collection. Therefore the key fundamentals set out in the ICC/ESOMAR Code (see Appendix 1) form the basis for this ESOMAR Guideline for Online Research.

While many of the technical and methodological issues involved in internet research have been clarified since this Guideline was last updated in 2005, the international legal framework governing the internet is still evolving meaning that online research operates in a less well defined legal framework than other forms of research, especially in a multi-country setting. The objective of this Guideline is to explain how to apply some of the fundamental principles of the Code in the context of the current legal and regulatory environments around the world and to support researchers in addressing legal, ethical and practical considerations in using new technologies when conducting online research.

ESOMAR regards it as vital to stress the distinction between market research and marketing. Market research is not a commercial communication and works within a less restrictive legal framework around the world. The distinction can be easily explained; personal data collected for market research are used only for research purposes and are not divulged for marketing directly to the individual or for other uses. See ESOMAR Guide Distinguishing market research from other data collection activities.

ESOMAR has worked closely with CASRO in developing this Guideline and in particular, the section on using technologies in research is based on and aligned with CASRO guidance.

The review of this document is still underway. The guidance on Access Panels in section 5.2 remains unchanged since first published but will be updated in the near future. It is also intended to add guidance on other relevant subjects.

1.1 Over-riding principles for online research

With laws varying from country to country and new possibilities emerging regularly, there should be **three over-riding guiding principles for online researchers.**

First, treat the respondent (or the person who is willing to participate in a survey) with respect. Researchers need to create a relationship with the public based on trust, respect and reciprocity by ensuring that people who participate in an online survey have a good experience.

Second, researchers must be sensitive to consumer concerns and remain mindful that market research depends for its success on public confidence. Researchers should avoid activities and technology practices that could undermine public confidence in the market research industry.

Third, researchers must remain diligent in maintaining the distinction between research and commercial activities such as direct marketing or advertisement targeting. Where researchers are involved with activities which use research techniques such as interviews but which are not intended solely for research purposes, they must not describe this as market, social or opinion research.

In addition researchers must adhere to the data protection requirements of Article 7c of the ICC/ESOMAR International Code on Market and Social Research which are as follows:

Personal information collected and held in accordance with this Code shall 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; and*
- *preserved no longer than is required for the purpose for which the information was collected or further processed.*

Researchers shall ensure that respondents' personal identity is withheld from the client. The researcher may communicate the respondent's identifiable personal information to the client, unless national provisions require stricter regulations, under the following conditions:

i) the respondent has explicitly expressed this wish and/or
ii) the respondent has given their explicit consent and
iii) on the understanding that no commercial activity (as defined in Article 1d of the ICC/ESOMAR Code of Market and Social Research) will be directed at them as a direct result of their having provided information.

2. ETHICAL ISSUES

2.1 Handling personal data

Data provided by respondents is confidential and the identity of respondents must be protected. The identity of respondents must not be revealed to the user of the information without respondents' explicit consent and the researcher must ensure that information is collected for specified research purposes and not used in any manner incompatible with these purposes (see Article 7 of the ICC/ESOMAR International Code). No personally identifiable information may be used for subsequent non-research purposes such as direct marketing, list-building, credit rating, fund-raising or other marketing activities relating to those individual respondents (see Article 1d of the Notes to the ICC/ESOMAR International Code).

2.1.1 Personal identifiers

A respondent's e-mail address or other personal identifiers (e.g. screen or user name or device identifier where it is recorded in the data) are personal data and must be protected in the same way as other identifiers.

If all data which could lead to the identification of an individual are removed from data records (including identifying serial numbers which link to a separate file of identity data) the data set no longer contains personal data and is no longer subject to the requirements of data protection and privacy laws or to early deletion.

2.2 Notifications and e-mail

Researchers must remain mindful of concerns about privacy and intrusion and not make unsolicited e-mail approaches to potential respondents even in countries where this is still permitted by the law unless individuals have a reasonable expectation that they may be contacted for research.

Researchers must reduce any inconvenience such an e-mail might cause to the recipient by clearly stating its purpose in the subject heading and keeping the total message as brief as possible.

The same requirement applies to other electronic messages (eg instant messaging, SMS etc). See section 4.4 on Interactive mobile.

2.2.1 Specific requirements

The general principle is that market researchers will not use unsolicited e-mails to recruit respondents for research purposes whether consumer or business-to-business.

Researchers are required to verify that individuals contacted by e-mail for research have a reasonable expectation that they will receive a contact for research. Such agreement can be assumed when ***all*** of the following conditions exist:

i. A substantive pre-existing relationship exists between the individuals contacted and the research organisation, the client or the list owners providing sample for the research (the latter being so identified);

ii. Individuals have a reasonable expectation, based on the pre-existing relationship, that they may be contacted for research;

iii. Individuals are offered the choice to be removed from future electronic contact in each invitation in a clear and distinct way and this must be free of charge and easy to implement;

iv. The invitation list excludes all individuals who have previously taken the appropriate and timely steps to request the list owner to remove them.

Researchers must not use any subterfuge in obtaining electronic addresses of potential respondents, such as collecting e-mail addresses from public domains or under the guise of some other activity, or using technologies or techniques to collect e-mail addresses without individuals' awareness.

Researchers must not use false or misleading return e-mail addresses when recruiting respondents over the internet.

Unsolicited survey invitation e-mails may be sent to business-to-business research respondents provided that researchers comply with points 3 and 4, as well as the anti-spam policies of their internet and e-mail service providers. This also applies to e-mail addresses of professionals whose details have been published in the public domain - e.g. lists of doctors or lawyers.

When receiving e-mail lists from clients or list owners, researchers must have the client or list provider confirm in writing and/or some durable form that individuals listed have a reasonable expectation that they will receive e-mail contact, as defined above.

It is good practice for researchers to keep copies of e-mails and other documents received from respondents agreeing to, or restricting, the use of or access to their personal information. This is a legal requirement in some countries, amongst others, all EU (European Union) member states, Argentina, Australia, Canada, New Zealand, and U.S. companies that participate in the U.S.-EU Safe Harbour Framework.

2.3 Privacy policies

Researchers must post a privacy policy statement on their online site. It must be clear, concise, and prominent.

2.3.1 Recommended content

The privacy policy must be made available as a link from every online survey and inform research participants how their personal information is used, kept secure and the conditions, if any, under which it may be disclosed to a third party. Some elements of the policy will be standard for all surveys (**see section A, standard elements for all privacy statements**). Other aspects will vary depending on the sampling methods used (**see section B, three additional elements**). There may also need to include upfront disclosure of privacy related information relevant to a particular survey in the invitation to participate, in addition to the more general statements in the privacy policy.

The order and wording of the privacy statement is a matter of choice. ESOMAR recommends that firms consider using a three layer privacy notice with the first layer giving a concise summary of the privacy policy, the second layer giving a brief overview of market research and the firm's privacy practices and a third layer providing the firm's comprehensive privacy policy. An example of a layered privacy notice is given in Appendix 2.

A. Standard elements for all privacy statements

Statement of **who** is doing the research. This could include a hyperlink to the research company home page for more information.

Who it is for: explanation that each survey will contain information about the identity of the company/organisation the research is being done for, unless there are good reasons for not providing this information. If the research company is providing a data collection service, the identity and contact details of the company receiving the personal data and therefore the "data controller", in EU terminology, should be provided. For further guidance on this issue see the Notes on how to apply the ICC/ESOMAR International Code note on Article 4.

Guarantee that in all circumstances identities of individual respondents and their answers will be treated as **confidential** and will be used only for research purposes unless the respondent explicitly requests or agrees to disclosure to a third party.

Will not mislead you: e.g. *"In obtaining your co-operation we will not mislead you about the nature of the research or the uses which will be made of the findings".*

Voluntary: e.g. *"As with all forms of market, social and opinion research, your co-operation is voluntary. No personal information is sought from or about you without your prior knowledge and agreement".*

Withdraw: e.g. *"You are entitled to withdraw at any stage of the interview, or subsequently, to ask that part or all of the record of your interview is destroyed or deleted. Wherever reasonable and practical we will conform to such a request".*

Identification and tracking technologies: clear statement of any technologies and processing related to the survey that are taking place. In addition to specific software that may be downloaded to a respondent's computer or device, most web surveys can detect information about the respondent without their knowledge such as browser type, user name and computer identification. Statements should say clearly what information is being captured and used during the interview (e.g. data collected for tracking purposes to deliver a page optimised to suit the browser)
and whether any of this information is being retained as part of the survey or administrative records.

Cookies: clear statement if they are being used, and if so, why e.g. *"We use cookies and other similar devices sparingly and only for quality control, validation and to prevent bothersome repeat surveying".* If cookies are being used, it would be advisable to include a reminder that the respondent has control over whether their computer accepts cookies e.g. *" Ensure your browser is configured so that you are alerted to the placement of all cookies. You can also delete cookies by adjusting your browser settings".*

Children: clear statement about how interviews with children will be carried out e.g. *"In research involving children, we will seek the verifiable permission of a parent, legal guardian or other person legally responsible for the child before an interview commences".*

How to contact us: e.g. *"We will provide a postal address, an e-mail address and/or a freephone number for respondents to contact us to discuss any concerns about a particular survey".*

Security measures: e.g. *"Our web site has security measures in place to protect the loss, misuse, and alteration of the information you provide to us. Only authorised employees have access to the information for data analysis and quality control purposes. If personal data are transferred to third parties, we ensure that they employ at least an equivalent level of security measures".*

Unsolicited mail: state policy not to send unsolicited mail or pass on e-mail addresses to others for this purpose.

Access to personal information[1]: how to access and if necessary correct information held on a respondent.

Where the data is held/processed: as many companies operate globally and may collect data in one country and process in another.

Registered address of the organisation.

Date the policy was last updated.

B. Three additional elements which will need to be included depending on the methodologies used to contact potential respondents.

i. Where the respondent is being **invited to join a panel** for market research purposes, or has already joined:

The sign up process: describe the registration process.

The panel database: describe information that will be stored in a research participant database, for panel management, control and sample selection and the process for updating it, deleting it or deleting all personal identifiers.

Frequency of contact: give an indication of what participation involves e.g. how often, for how long.

Password identity system: if it is used, describe how it works and the security it offers.

Opt in and opt out policies for communications other than surveys, such as panel maintenance or reward schemes. State what communications will be sent, which are optional and clarify any potential communications on behalf of third parties.

Reward: explain any reward scheme and if this forms the basis for a contract.

ii. Where the researcher has obtained **a list of e-mail addresses** in order to send invitations to participate in a survey:

Source of information: clear statement of where the e-mail address came from or that this will be included in the information given in the survey itself. A statement that the list provider has verified to the researcher that the individuals listed have a reasonable expectation that they will receive e-mail contact.

Spamming: will not knowingly send e-mail to people who have not consented to helping in research and must include a mechanism for the researcher to remove their name from future surveys or notify the provider of the e-mail list.

Password identity system: if it is used describe how it works and the security it offers.

Stop and start interview process: if this is possible explain how, and any information stored to allow it.

iii. **Intercept surveys** where the respondent is selected as a 1-in-n sample of visitors to a web site or similar technique:

[1] *Note to researchers: In Europe, Australia, Canada, New Zealand and other jurisdictions that have comprehensive privacy laws, individuals have a statutory right to access their personal information that is held by organisations, subject to certain conditions. Individuals' access rights also apply to U.S. companies that participate in the U.S.-EU Safe Harbour Framework.*

Explain intercept technique: e.g. random selection.

Password identity system: if it is used, describe how it works and the security it offers.

Stop and start interview process: if this is possible, explain how, and any information stored to allow it.

Invisible processing: describe any invisible processing used to make the intercept or re-direct respondents to the survey.

See Appendix 2 – Example privacy policy

2.4 Children and young people

Researchers must be sensitive to concerns of parents, consumer groups and legislators about the potential exploitation of children and young people on the internet. All reasonable measures must be taken to ensure verifiable and explicit permission is obtained from a parent or legal guardian to invite a child to participate in a research survey although it is recognised that the identification of children and young people is not possible with certainty on the internet at this time.

2.4.1 Obtaining permission

Researchers must observe all relevant laws and national codes specifically relating to children and young people noting that the age definition for children varies from country to country. Where there is no specific national definition, the ESOMAR Guideline on Interviewing Children and Young People recommends those aged under 14 should be treated as "children" and those aged 14-17 as "young people" since market research is founded in the social sciences and recognizes different stages of mental and psychological development. [2]

Before interviewing children, researchers must ensure that permission is obtained from a parent, legal guardian or other person legally responsible for the child (hereafter referred to as 'parent').

Questionnaires on websites aimed at children must require a child to give their age before any other personal information is requested. If the age given is below the nationally agreed definition of a child, the child should not be invited to provide further personal information until the appropriate permission has been obtained. This notice must be clear and prominent, include an explanation of the subject and refer to the fact that permission will be verified where relevant. A request to the parent for their permission must be provided on the research provider's website or e-mailed to a parent.

Where personal information collected from children will only be used for research purposes and no personal data will be passed on for any other purpose, permission can be a return e-mail from the parent or other suitable method that is in compliance with the relevant laws and national codes.

Reasonable steps must be taken to validate that they actually have agreed by following up with an e-mail, letter or phone call for example, having asked the child to provide their parent's contact details so that their permission can be sought.

Prior parental permission is not required to:

- Collect a child's or parent's e-mail address solely to provide notice of data collection and request permission.
- Collect a child's age for screening and exclusion purposes. If this screening leads to the decision that a child does qualify for interview, parental permission must then be sought to continue with the interview.

In ensuring that all reasonable precautions are taken to ensure respondents are not adversely affected as a result of participating in a research project, asking children and young people questions on topics generally regarded as sensitive must be avoided wherever possible and in any case handled with extreme care.

Personal information relating to other people (for example, parents) must not be collected from children.

Where researchers are setting out to recruit children for repeated surveys they should consider:

- Recruiting parents with children of the required age and then managing the research process with the agreement and monitoring of the activity by the parent.
- Enabling password protection of surveys so that the entry of a password known only by the parent is required which means the parent must agree to provide it before the child can proceed in the research.

Where necessary, researchers should consult their national research association or the ESOMAR Guideline for advice.

[2] *Note that the locally defined age of "children" varies in different countries, and is, for instance, under 16 in the U.K.*

3. REGULATORY ISSUES

3.1 Personal data and IP addresses

Data privacy legislation applies only to personally identifiable data, not to data sets where it is impossible to identify any individual. Under these laws data subjects normally have a right of access to data held in a personally identifiable form, to view records being held in their name and to request corrections if there are errors. This right of access no longer applies once the personally identifiable elements have been removed from the data set.

The inclusion in a data set of, for example, a name, address, e-mail address or phone number would create personally identifiable data. It might also occur if there were an exact geographic location or postal code that could be combined with other information in the data set. Researchers must take care to ensure that data sets collected for market research that contain personally identifiable data are kept securely and are only used for market research purposes.

An IP address is necessary to link to the internet and is routinely captured by websites and software running on servers and personal computers connected to the internet. In general, the user is unable to prevent the capture of the IP address from taking place. An IP address might constitute personal data in combination with other identifiable data but there is no international consensus about the status of IP addresses. They can often identify a unique computer or other device, but may or may not identify a unique user. Accordingly, ESOMAR requires compliance with the relevant national and/or local law and/or regulation if it classifies IP addresses as personal data.

3.2 National jurisdiction

The ICC/ESOMAR International Code is to be applied against the background of applicable law and of any stricter standards or rules that may be required in any specific market. However, data privacy requirements and responsibilities are still being defined on an international level.

ESOMAR's advice to researchers is to consider the respondent's point of view and that, in participating in surveys, respondents would assume that the legal requirements of their own country would be met. Where it is possible to know the respondents' country of residence, then the researcher should follow the legal requirements of that country noting that requirements in the EU are not exactly the same, for example, both Germany and Italy have stricter requirements than other member states.

3.2.1 Remote data collection and data transfer

Researchers are advised to clarify which country(ies) are intended for the research study, especially if this differs from the country where the research company is established. The language of the website or questionnaire will play a role in clarifying the target country(ies). They can also be specified in the privacy policy which should comply with the regulations of where the research company is established.

Respondents should be informed of the law(s) under which the data is being collected on the front page of the survey at the point where respondent consent is being requested and this will also clarify conditions in circumstances where the respondent's country of residence is not known, for instance in worldwide customer satisfaction surveys or in monitoring a website where respondents could be located anywhere. For non-panel approaches (including web intercept) the aforementioned practice is most appropriate. For panels, it is common practice to inform respondents of the law in effect via the panel registration and privacy policies.

In the EU, ESOMAR requires the researcher collecting the data (the data controller) to comply with the law of the country in which they are established and, if collecting data in several countries, also to comply with the laws of those countries in which data collection is taking place. EU law in this area is still being clarified and ESOMAR will monitor developments.

Before personal data is transferred from the country of collection to a third country, the researcher must ensure that the data transfer is legal, and that all reasonable steps are taken to ensure adequate security to maintain the data protection rights of individuals. This also applies if using a "remote" server in a different country to collect data from the respondent or it is processed in an international "cloud".

The researcher must explain this process in their privacy policy (see recommended content for privacy policy and example privacy policy) and provide appropriate safeguards to protect personal data when asking the respondent for permission for the data transfer.

The use of standard contractual clauses which businesses can use to ensure adequate safeguards when personal data is transferred from the EU to non-EU countries is recommended, for instance those developed by the European Commission and the ICC.

3.3 Registration

In countries with data protection legislation, data controllers are usually required to register with the authorities. Researchers should register their activities with the appropriate authorities. For advice about the impact of data protection laws on market research in countries like Germany, UK and USA, see section 6.

3.4 Security

Researchers and their subcontractors must take adequate precautions to provide the highest level of security when collecting personally identifiable data, and in particular any sensitive data which may be defined in data protection legislation as requiring particularly careful management (see section 6).

Researchers must also take reasonable steps to ensure that any confidential information provided to them by clients or others is protected (e.g. by firewall and password controls) against unauthorised access.

Clients must be fully informed and mindful about the potential risks of posting details of confidential information in internet surveys and be required to implement strict security procedures. Concepts and ideas generally cannot be secured by technological means alone and statements once distributed, even when protected by non-disclosure agreements, are easily forwarded and effectively impossible to remove from circulation once released.

3.4.1 Managing security

Researchers must use security technologies to protect the personal data collected or stored on websites or servers, using reliable encryption systems such as Secure Socket Layer (SSL) encryption mode or equivalent level security. If the relevant national law requires, data “at rest” (typically defined as all data in storage but excluding any data that frequently traverses the network or that which resides in temporary memory) should also be encrypted at a suitable level.

Data security is also important to prevent unauthorised access to, manipulation of or disclosure of personally identifiable data including during data transfer. The research provider must have clear policies and procedures to manage security. Access to data should be restricted and allowed only on a need to know basis. The researcher
should ensure that all relevant managers and key staff handling such sensitive data have signed to confirm they will follow ICC/ESOMAR Code and not disclose personal data.

If the temporary storage of the data being collected takes place on a server that is operated by a sub-contractor or service provider, the researcher must place sub-contractors under a contractual obligation to take the necessary precautions to prevent unauthorised access while the data is stored or during data transfer. The identifiable data held by the service provider must be deleted at the earliest possible time.

4. USING ONLINE IDENTIFICATION AND TRACKING TECHNOLOGIES IN RESEARCH

Online identification and tracking technologies have developed rapidly over the past few years on a global scale. Whilst many of these technologies are designed to improve the computer user experience, they have led to close scrutiny from privacy groups who are concerned about the potential for organisations or individuals to identify and monitor individuals online without their knowledge.

Online identification and tracking technologies developed for market, opinion and social research are applied to improve the integrity of research panels and sampling techniques, since the researcher and the participant will usually only interact online.

ESOMAR, working in close cooperation with CASRO, and the global research industry, has established clear guidance on the conduct of market, social and opinion research using online technologies and, by doing so, aims to promote professional standards, best practices, and respectful relationships with research participants.

4.1 Identification and tracking technologies for market, social and opinion research

Identification and tracking technologies are technologies used to identify, validate and track respondents or respondent activity for research on the internet. Uses of these technologies can include ad tracking, survey quota control, fraud prevention and behavioural research. The terms spyware and malware are widely used to describe the unacceptable use of online tracking and identification technologies. Market social and opinion research must not use technology in such a way that it would be classified as spyware or malware. This section sets out acceptable and unacceptable uses of this technology as well as guidance on specific technology types.

4.1.1 Specific technologies

Identification and tracking technologies for research include the following:

Cookies
Cookies are small text files stored on a computer by a website that assigns a numerical user ID and stores certain information about your online browsing. Cookies are used on survey sites to help the researcher recognise the respondent as a prior user as well as for other survey control or quality functions. The data stored on cookies is not personalised and they can be rejected or deleted through browser settings.

Researchers must include clear, concise and conspicuous information about whether they use cookies and if so why (see section on privacy policy guide). If cookies are used, the researcher must ensure that a description of the data collected and its use is fully disclosed in the research organisation's privacy policy.

EU legislation passed in 2009 to be translated into national legislation by 2011, states that a cookie can be stored on a user's computer, or accessed from that computer, only if the user "has given his or her consent, having been provided with clear and comprehensive information". An exception exists where the cookie is "strictly necessary" for the provision of a service "explicitly requested" by the user ensuring that users of their websites were provided with "clear **and** comprehensive information about the purposes of the storage of, or access to, that information" **and** ultimately, provide the user with the opportunity to refuse such storage of, **and**/or access to, that information. Researchers conducting research in the EU should consult updates on whether they are required by national legislation to seek consent for cookies.

Researchers collecting panel data and tracking respondents behaviour across the internet need to cover this in their privacy statement (see section on panel data) and should also explain this activity on the sign up page for the panel in order to be sure that respondents are completely clear about the information being collected from them.

Flash cookies
Flash cookies originate from coding found in Adobe's Flash media player, an application which is used by the vast majority of commercial websites that feature animations or videos.

If used in a research technique, researchers must disclose the use of this information, provide details on how to remove them in their privacy policy (see section on privacy policy guide) and seek respondents' prior consent. In addition, other new techniques are being developed such as HTML5 local storage features that cannot be easily deleted.

Device ID (also referred to as Digital Fingerprinting or Machine ID)
These are technologies that deploy an algorithm that analyses a large number of technical characteristics and settings to generate a unique identifier that can identify a specific computer, producing a device-ID or a machine ID.

Active agent technologies
Active agent technologies for research are software or hardware devices that capture respondent's behaviour in background mode, typically running concurrently with other activities. They include:

- Direct to desktop software downloaded to a user's computer that is used solely for the purpose of alerting potential survey respondents downloading survey content or asking survey questions. It does not track data subjects as they browse the internet and all data collected is provided directly from user input;
- Tracking software that can capture the data subject's actual online behaviour such as web page hits, web pages visited, online transactions completed, online forms completed, advertising click-through rates or impressions, and online purchases. This software also has the ability to capture information from the data subject's e-mail 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 occurs without the data subject's full knowledge and opt-in consent.

The use of spyware by researchers is strictly prohibited.

4.1.2 Disclosure for identification and tracking technology

Disclosures regarding the use of identification and tracking technologies must be transparent and made before or at the time of collection. For individual projects, such disclosures can form part of the recruitment invitation and a project-specific privacy policy could apply. If a particular technology is used across multiple or all projects, disclosures regarding the technology should form part of the research organisation's general privacy policy for online respondents. Hyperlinks to project-specific and/or general privacy policies should be readily accessible to respondents (e.g. in survey invitations and/or on the landing page of online surveys).

Examples of disclosure statements are provided in Appendix 2 for the use of:
Cookies
Flash cookies
Cookies and software applications for tracking
Device/machine identification

4.2 Practices that research organisations should adopt

The following are practices researchers who deploy identification and tracking technologies for research should adopt. Researchers who adopt these practices and do not engage in any of the practices set forth in unacceptable practices (Section 4.3 of this guideline) will not be considered users of spyware.

Transparency is critical. Researchers must disclose information about identification and tracking technologies and other software in a timely and open manner with data subjects. This communication must provide details on how the researcher uses and shares the data subject's information

i. Only after receiving permission from the data subject (parent or legal guardian's permission for children) should any research software be downloaded onto the individual's computer, PDA or other device.[3]

ii. Researchers must clearly communicate to the respondent the types of data if any, that are being collected and stored by a particular identification and tracking technology.

iii. Disclosure is also needed to allow the respondent to easily uninstall research software without prejudice or harm to them or their computer systems.

iv. Personal information about the respondent must not be used for secondary purposes or shared with third parties without the respondent's opt-in consent.

[3] *This requirement and many of the others in this section do not apply to computers or data capture equipment provided to the respondent by the researcher, where the researcher remains the owner and controller of the device.*

v. Researchers must ensure that participation is a conscious and voluntary activity. Accordingly, incentives must never be used to hide or obfuscate the acceptance of identification and tracking technologies for research.

vi. Researchers must ensure there is a method to receive queries from end-users.

vii. On a routine and ongoing basis, consistent with the stated policies of the research company, data subjects who participate in the research panel should receive clear, periodic notification that they are actively recorded as participants, so as to ensure that their participation is voluntary. Researchers must provide to respondents who participate in a research panel, a clearly defined method to uninstall the researcher's tracking software without causing harm to the data subject.

viii. When installing updates to software to correct errors, security problems or new releases which do not increase the scope of personal data that is collected, if there is no response to notification after a reasonable time (30 days), it can be assumed that the participant has agreed. This assumption should be covered in the privacy statement. If the researcher decides to reduce the 30 day notification period for a specific application, this must be explicitly mentioned in a prominent place on the website.

Responsible handling of data is critical. Researchers must take steps to protect information collected from respondents.

i. Personal or sensitive data must not be collected unless consent is obtained. If consent is not obtained and collection is unavoidable, the data should be destroyed immediately. If this is not possible, it must receive the highest level of data security and must not be accessed or used for any other purpose.

ii. Researchers must establish safeguards that minimise the risk of data security and privacy threats to the data subject.

iii. It is important for researchers to understand the impact of their technology on end-users, especially when their software downloads in a bundle with other comparable software products.

iv. Researchers must make all reasonable efforts to ensure that these products (whether they are free of charge or not) are safe, secure and do not cause undue privacy or data security risks.

v. Researchers must also be proactive in managing distribution of the software and vigorously monitor their distribution channel and look for signs that suggest unusual events such as high churn rates.

4.3 Unacceptable practices

Following is a list of unacceptable practices that researchers must strictly forbid or prevent. Researchers are considered to be using spyware when they fail to adopt all of the practices set forth below:

i. Downloading software without obtaining the data subject's consent;

ii. Downloading software without providing full notice and disclosure about the types of information that will be collected about the data subject, and how this information may be used. This notice must be clear, concise and conspicuous;

iii. Collecting information that identifies the data subject without obtaining consent;

iv. Using keystroke loggers without obtaining the data subject's opt-in consent;

v. Installing software that modifies the data subject's computer settings beyond that which is necessary to conduct research;

vi. Installing software that turns off anti-spyware, anti-virus, or anti-spam software or seizes control or hijacks the data subject's computer or device;

vii. 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;

viii. Installing software that is hidden within other software that may be downloaded or that is difficult to uninstall;

ix. Installing software that delivers advertising content, with the exception of software for the purpose of advertising testing;

x. Installing upgrades to software without notifying users and giving the participant the opportunity to opt out;

xi. Changing the nature of the identification and tracking technologies without notifying the user;

xii. Failing to notify the user of privacy practice changes relating to upgrades to the software;

xiii. Tracking the content of the data subject's e-mail;

xiv. If the respondent's browser is set to private mode, the researcher must not track behaviour unless opt-in consent is obtained;

xv. When the respondent is on a site which is set to secure linkage (i.e. SSL site), the researcher must not collect personal data unless opt-in consent is obtained from the respondent.

4.4 Interactive mobile devices and smartphones

Interactive mobile devices and smart phones are able to combine the characteristics of a mobile phone and an internet browser. ESOMAR has published guidelines on both online research (this document) and research using mobile phones. The appropriate guide to follow for interactive mobile devices depends on whether the researcher contacts the respondent using the facilities of a mobile phone (i.e. calling them or sending SMS messages) or using internet facilities (i.e. email, web browser link or downloaded application). If a combination of the two is used, e.g. mobile phone to contact and internet browser to respond, then the appropriate parts of both guidelines should be applied.

4.4.1 Using interactive mobile devices

Contacting
If contacting people using online methodologies, researchers must not make unsolicited approaches by e-mail or other messages (eg instant messaging, SMS etc.) to potential respondents even in countries where this is still permitted by the law. They are required to verify that individuals contacted by such means for research have a reasonable expectation that they will receive a contact for research. See section 2.2 on Notifications and e-mail.

Security and downloads
Where researchers install apps on mobile interactive devices, they should comply with section 4.1.1 and 4.1.2 of this guideline. Researchers must offer respondents an appropriate channel and mechanism for giving permission and a place where they can read more about the privacy policy. In addition to complying with section 3.4, researchers should ensure that any data stored locally on the device is secure and unavailable to others should the device be stolen or used by another person. This could be achieved by data encryption.

Cost to respondent
Respondents using mobile interactive devices to take part in surveys may incur air-time, roaming or data costs in so doing. If possible, the researcher should design the study so that the respondent incurs no cost. If this is not possible, the researcher must be prepared to compensate respondents for their costs. Where interactive mobile respondents are added to a panel or sampling database the issue of cost and compensation should be agreed at the "sign up" stage.

Appropriate design
When contacting respondents known to be using mobile interactive devices, the researcher should ensure that the survey is presented in a suitable format that is optimised across devices which are likely to be viewed by participants. Respondents should also be given the opportunity to opt out of that survey.

Privacy policy
Because of space limitations on the screen of mobile interactive devices it may be difficult to display a full privacy policy. Researchers must apply a suitable solution and take appropriate steps to minimise cost and maximise convenience in accessing the relevant information. For instance, researchers should provide a weblink to their privacy policy with the shortest possible url, and provide a freephone number and/or a postal address.

Location data and GPS
It is now possible to capture additional data from interactive mobile devices and smartphones such as real time location data. ESOMAR's Guideline on Passive Data Collection addresses this issue. The researcher must have the respondent's permission before processing it.

5. METHODOLOGY ISSUES

5.1 Online sample

There are a number of different ways to recruit online samples and these require different forms of consent (see section 2.3 on privacy policies). Panel members' personal data is held by the panel provider, whereas other forms of sampling do not normally require the personal data to be retained by the research service provider. If it is intended to store individuals' personal data, appropriate consent must be obtained either before or at the time of collection.

5.2 Access Panels

This section is currently under review and will be inserted here when complete. Meanwhile see the existing guide, 26 questions which is in the process of being updated.

5.3 Technical details

The ICC/ESOMAR Code of Conduct (Articles 4d and e) requires researchers to provide full technical details of the survey methodology used in carrying out a project; online research may well have complex methodologies and sampling strategies. This makes it even more important that the technical details are reported in such a way that a study can be replicated.

The ESOMAR Guideline on the Mutual Rights and Responsibilities of Researchers and Clients sets out the requirements for the technical reporting of research projects required by the ICC/ESOMAR Code. This guidance applies to all research projects including online research.

6. DEFINITIONS AND USEFUL SOURCES OF INFORMATION

Three key concepts, researcher, personal data and consent are addressed below for the purposes of this guideline:

Researcher: is defined in the ICC/ESOMAR International Code as any individual or organisation carrying out, or acting as a consultant on, a market research project, including those working in client organisations.

Personal data means any information relating to an identified or identifiable natural person i.e. a private individual as opposed to a corporate or other comparable entity. 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.

Sensitive personal 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, trade union membership. In the U.S., personal health-related information, income or other financial information, financial identifiers and government-issued or financial identity documents are also regarded as sensitive.

Consent means the freely given and informed agreement by a data subject to the collection and processing of their personal data. In market research, this consent is can be based on the fact that the respondent voluntarily provides answers in a survey having been provided with clear information about the nature of the data being collected, the purpose for which it will be used and the identity of the person or organisation holding the personal data. The respondent may withdraw their consent at any time by refusing to cooperate in an interview or research project.

Unambiguous consent is used in the EU Directive applying to the processing of personal data in general. However, as the term unambiguous consent is not recognised outside the EU, the terms 'consent' is used in this guideline.

Key relevant legislation

The EU Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) regulates the processing of personal data within the EU. All 27 EU Member States have transposed the Directive and enacted their own national data protection legislation.

The EU Directive on privacy and electronic communications (officially 2009/136/EC) requires prior consent for unsolicited commercial electronic communications, and covers SMS text messages and other electronic messages received on any fixed or mobile terminal. It also requires end user consent to the storing of cookies on their computer after having been provided clear and

comprehensive information on the purposes and role of cookies. This Directive tightens the existing e-Privacy Directive, 2002/58/EC and its impact will depend on its implementation by EU Member States into national law required by 2011, as well as the influence of the European Commission.

Canada – Personal information protection and electronic documents act
Personal Information means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organisation.
Note: A workplace e-mail address is considered personal information under PIPEDA. Sensitive personal information is not defined in the law.

U.S. Federal laws
Data protection laws in the U.S. at the federal level are sector-specific as, currently, no single, comprehensive, national privacy law exists that applies to all private sector organisations.

Two sector-specific privacy laws apply to certain organisations in the financial and healthcare sectors: The Gramm-Leach-Bliley Act (GLB) and Health Insurance Portability and Accountability Act (HIPPA).

When researching children the Children's Online Privacy Protection Act (COPPA) applies.

U.S. State laws regarding data security breaches
California Senate Bill 1386 – the first security breach notification law in the U.S. defines personal information to mean:

An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
1. Social security number.
2. Driver's license number or California Identification Card number.
3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Useful sources

The following provide helpful and relevant material for the online researcher:

ACE Association Collaborative Effort: An up to date set of definitions for key internet research concepts has been developed here;

AMSRO Market and Social Research Privacy Code and the Market and Social Research Privacy Principles;

COPPA Children's Online Privacy Protection Act;

CASRO Code of Standards and Ethics for Survey Research, Section 3. Internet Research;

ADM Declaration for the Territory of the Federal Republic of Germany concerning the ICC/ESOMAR International Code of Market and Social Research and guidelines;

DMA Code of Practice for Commercial Communications to Children Online;

Guidelines for Online Surveys (Germany) undersigned by ADM, ASI, BVM, DGOF;

MRS Code and Guidelines for Researching Children and young people;

U.S.-EU & Swiss Safe Harbour Frameworks: In order to bridge the different privacy approaches of the U.S. and the EU and provide a streamlined means for U.S. organisations to comply with the EU Directive when transferring personal data from the EU to the U.S., the U.S. Department of Commerce in consultation with the European Commission developed a Safe Harbour framework to provide the information an organization should need to evaluate and then join the Safe Harbour;
European Commission: Model contracts for transfer of personal data from the EU;

ISO 26362:2009: Press release on access panels in market and opinion research – Vocabulary and service requirements;

ISO 20252:2006: Market, opinion and social research - Vocabulary and service requirements.

Project Team

John O Brien, consultant to ESOMAR Professional Standards Committee (Chair Project Team)
Reg Baker, COO, Market Strategies
Diane Bowers, ESOMAR Professional Standards Committee member and President of CASRO
Mike Cooke, Global Director, Online Development, GfK NOP
Jonathan Jephcott, Executive Vice President, ViewsNet, Synovate
Kathy Joe, Director, Professional Standards and Public Affairs, ESOMAR
Kees de Jong, CEO, Survey Sampling International
Peter Milla, Consultant to CASRO
Adam Phillips, Chair of ESOMAR Professional Standards Committee and Legal Committee
Reneé Smith, Chief Research Officer, Kantar
David Stark, Vice President, Compliance and Privacy Officer, GfK
Kevin Umeh, Past CEO at Cint USA

Additional guidance

Members who are unsure about the application of the Guideline in specific circumstances can seek advice by contacting the Professional Standards Committee, professional.standards@esomar.org or ESOMAR, Eurocenter 2, 11th floor, Barbara Strozzilaan 384, 1083 HN Amsterdam, The Netherlands.

APPENDIX 1 - Key fundamentals of the ICC/ESOMAR Code

1. Market researchers shall conform to all relevant national and international laws.
2. Market researchers shall behave ethically and shall not do anything which might damage the reputation of market research.
3. Market researchers shall take special care when carrying out research among children and young people.
4. Respondents' cooperation is voluntary and must be based on adequate, and not misleading, information about the general purpose and nature of the project when their agreement to participate is being obtained and all such statements shall be honoured.
5. The rights of respondents as private individuals shall be respected by market researchers and they shall not be harmed or adversely affected as the direct result of cooperating in a market research project.
6. Market researchers shall never allow personal data they collect in a market research project to be used for any purpose other than market research.
7. Market researchers shall ensure that projects and activities are designed, carried out, reported and documented accurately, transparently and objectively.
8. Market researchers shall conform to the accepted principles of fair competition.

APPENDIX 2 – Example Privacy Policy

The example given below provides a framework for a privacy policy. The text should not be treated as comprehensive or up-to-date with all national laws or local requirements. It is the responsibility of the researcher to ensure that their policy meets national requirements in force at the time and in the countries in which they are working.

The policy is divided into three main sections a concise top level statement on how privacy will be protected and data used, a second level general introduction which describes the purpose and general principles and third, a detailed section covering all aspects of how the researcher treats personal data.

EXAMPLE:

Level 1

Thank you for taking part in our research project.

1 We promise to protect your privacy and treat the information you give us as confidential.
2 The information you provide will be used only for research purposes.
3 We will not release your personal information to any third party without your consent.
4 We will never try to sell you anything and we will never sell your personal data to anyone. That is not our business. We are not telemarketers or direct marketers. We are market researchers interested only in your opinions and behaviour.
5 Your decisions about participating in a study, responding to specific questions, or discontinuing participation will be respected without question.

Click here for more information about market research (Level 2)
Click here for a comprehensive statement of our privacy policies (Level 3)

Level 2

Your privacy is important to us

Market, survey and opinion research serves an important function in society. Businesses and governments make better decisions through survey research. As a survey participant, your opinions help companies develop new products, make existing ones better, and improve customer service. Political organisations and governments also rely on survey research to advance laws and policies that the public wants or needs.

When you participate in research conducted by our firm, you can be assured that we will protect your privacy. Occasionally, we may re-contact you to validate your responses. We will never misrepresent ourselves or what we are doing.

We have developed rigorous privacy standards that are set out in our detailed privacy policy. Several members of our firm's professional staff belong to ESOMAR, the world organisation for enabling better research into markets, consumers and societies. ESOMAR sets professional standards to which our firm adheres, and which also protect your privacy.

If you have any privacy questions or concerns, please contact our Privacy Officer via e-mail at (insert e-mail address) by telephone at (insert free phone number) or by mail (insert mailing address).

Level 3

Privacy Policy

Date created: (*insert date*)

Last revised: (*insert date*)

Note to researchers: Some U.S. states require website privacy policies to include the above information. It is good practice to include the last revised date so that consumers are informed when companies make substantive changes to their privacy statements.

1. The information that we collect

When our firm conducts online research, our invitations and questionnaires clearly identify us and explain the purpose(s) of our contact.

When we contact you, we generally do so for one of the following purposes:

1. To invite you to participate in survey research;
2. To conduct a survey research interview with you;
3. To validate answers you gave in a recent survey we conducted;
4. To update and to ensure that our records of your personal information are correct. (*applicable only to panels).*

Occasionally, we may contact you for one of these other purposes:

1. To notify you if you have won a prize draw that we sponsored (*if a relevant incentive*);
2. To ask for your permission to use your personal information for a purpose that was not explained to you when we first collected your personal information.

When you participate in our research, we may ask you for your personal opinions, as well as demographic information, such as your age and household composition. You may refuse to answer certain questions or discontinue participation in a study at any time. If you join our internet research panel, you may rescind your membership at any time by following the opt-out instructions that we include in every e-mail that we send.

We never knowingly invite children under the age of (*insert age depending on national industry codes and pertinent laws*) to participate in research studies without taking measures to ensure appropriate parental consent.

2. Confidentiality of survey responses and contact information

We combine your survey responses in a given survey with the responses of all others who participate and report those combined responses to the client that commissioned the study. We will never intentionally report your individual survey responses, except as described below.

Your survey responses may be collected, stored or processed by our affiliated companies or non-affiliated service providers, both within and outside (*insert country where firm is located*). They are contractually bound to keep any information they collect and disclose to us or we collect and disclose to them confidential and must protect it with security standards and practices that are equivalent to our own.

In addition to keeping your survey responses confidential, we will never sell, share, rent or otherwise intentionally transfer your name, address, telephone number or e-mail address to our clients, other market research companies, direct marketing companies or anyone else.

The only exceptions when we may disclose your personal information or survey responses to third parties are as follows

1. You request or consent to sharing your identifying information and individual responses with the third parties for a specified purpose;

2. In accordance with the ESOMAR guidelines, we provide your responses to a third party who is contractually bound to keep the information disclosed confidential and use it only for research or statistical purposes;

3. In the rare but possible circumstance that the information is subject to disclosure pursuant to judicial or other government subpoenas, warrants, orders or for similar legal or regulatory requirements.

3. Use of cookies, log files and other technologies on our website

Cookies are small text files stored on your computer by a website that assigns a numerical user ID and stores certain information about your online browsing. We use cookies on our survey site to help us provide you a better experience and to provide quality control and validation functions. No personal information is stored on any cookie that we use.

(May be applicable to panels) Some of the cookies that we use on this site are required because they identify you as a valid member of our panel, and they protect access to your profile and account information. The privacy settings of your browser must be configured to allow cookies from (*insert website* URL) or you will not be able to register on the (*insert website* URL) panel or access the Members Area of this site. If you wish, you can adjust your browser's privacy settings to delete cookies upon exiting web sites or when you close your browser.

This site uses Flash Local Shared Objects (LSO), also known as "Flash cookies," to store some of your preferences, to display content based upon what you view, to personalize your visit, to combat fraud that endangers the quality of research, or to otherwise track your behaviour and activities across multiple visits to the site. We use Flash cookies strictly for research purposes only.

Flash cookies are different from browser cookies because of the amount and type of data stored and how the data are stored. The latest versions of popular browsers now allow internet users to manage Flash cookies using browser privacy settings or downloading add-ons..

If your browser does not support these features, then you canmanage privacy and storage settings for Flash cookies or disable their use entirely by visiting Macromedia's website, the manufacturer of Flash Player, at the following link:

Adobe - Flash Player: Settings Manager:
http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html

Note, researchers in the EU are recommended to consult section 4.1.1 relating to EU legislation and possible requirements for consent to cookies being placed unless the cookie is strictly necessary for the provision of a service explicitly requested.

(Applicable to behavioural tracking research) We use optional cookies, both browser and Flash-based, (insert "software applications" if this applies to your panel) for conducting advertising and website research. These cookies are available only to members of our panel who have explicitly agreed to participate in our behavioural tracking research programme. The cookies keep track of certain online advertisements and web pages that you see, including how frequently the online content that we are measuring is viewed by your computer. Only a small number of ads or websites are measured through this research programme and the information we collect is used strictly for research purposes. No commercial messages or communications will be directed to you as a result of taking part in this research. Full details about this programme are available to you when you are logged into our site including instructions on how to discontinue your participation at any time.

Like most web sites, we gather certain information automatically and store it in log files. This information includes IP (Internet Protocol) addresses, browser type, internet service provider (ISP), referring/exit pages, operating system, date/time stamp and clickstream data. We use this information to analyse trends, to administer our site, to track users' movements around our site and to gather demographic information about our user base as a whole. To protect against fraud, we may link this automatically-collected data to information submitted at (*insert research firm's* URL).

(Applicable to Device ID) Device Identification technologies assign a unique identifier to a user's computer to identify and track the computer. (*insert company name*) does not use Device identification (also known as machine id or digital fingerprinting) technology to collect personal information or track the online activities of computer users. We use the technology to assist our clients in ensuring the integrity of survey results. The technology analyses information and data obtained from your computer's web browser and from other publically available data points, including for example the technical settings of your computer, the characteristics of your computer, and your computer's IP address. This data is used to create a unique identifier assigned to your computer. The unique identifier is an alpha-numeric id which we retain. We do not retain the information analysed by the technology to create the unique identifier. The technology does not disrupt or interfere with your use or control of your computer and it does not alter, modify or change the settings or functionality of your computer.

In furtherance of our efforts to assist clients in protecting and ensuring the integrity of survey results, we:

a. may link or associate your unique identifier to you and any of the information you provide to us;
b. may share your unique identifier with our clients and with other sample or panel providers; and
c. may receive or obtain a unique identifier linked to you from a third party, including without limitation a sample or panel provider or a client of our firm.

Any unique identifier(s) linked to a specific individual will be protected in accordance with this privacy policy. We shall use and distribute the technology in a professional and ethical manner and in accordance with our privacy policy, any statements and/or disclosures made by our firm to you, and applicable laws and industry codes.

In the event that we discover or learn of any unethical conduct in connection with the use of the technology, or that the technology is being used in a manner that is inconsistent with the statements and/or disclosures made by us to respondents or in violation of applicable laws and codes, we will take immediate action to prohibit such unethical conduct and to ensure the proper administration of the technology.

4. Security of personal information

We inform our employees about our policies and procedures regarding confidentiality, security and privacy, and we emphasise the importance of complying with them. Our security procedures are consistent with generally accepted commercial standards used to protect personal information.

We may transfer personal information to affiliated companies or non-affiliated service providers for research-related purposes, such as data processing, and fulfilment of prize draws or other incentives. We require these companies to safeguard all personal information in a way that is consistent with our firm's measures and as regulated by law. We follow generally accepted industry standards to protect the personal information submitted to us, both during transmission and once we receive it.

5. Accuracy of personal information

(insert company name) makes reasonable efforts to keep personal information in its possession or control, which is used on an ongoing basis, accurate, complete, current and relevant, based on the most recent information available to us. We rely on you to help us keep your personal information accurate, complete and current by answering our questions honestly.

6. Access to personal information

Note to researchers: *In Europe, Australia, Canada, New Zealand and other jurisdictions that have comprehensive privacy laws, individuals have a statutory right to access their personal information that is held by organisations, subject to certain conditions. Individuals' access rights also apply to U.S. companies who participate in the U.S.-EU Safe Harbour Framework.*
To request access to personal information that we hold about you, we require that you submit your request in writing at the e-mail address or postal address shown below (in How to reach us). You may be able to access your personal information and correct, amend or delete it where it is inaccurate, except as follows:

1. Providing access to your personal information would be likely to reveal personal information about others;

2. Disclosing the information would reveal the confidential commercial information of *(insert name of firm)* or its clients.

3. The burden or expense of providing access would be disproportionate to the risks to your privacy in the case in question.

We will endeavour to provide your requested personal information within 30 days of receiving your access request. If we cannot fulfil your request, we will provide you with a written explanation of why we had to deny your access request.

7. Notification of material changes to this policy

If we make a material change to this policy or our privacy practices, we will post a prominent notice on this site for 30 calendar days prior to the implementation of the material change and describe how individuals may exercise any applicable choice. Following the implementation of the material change, we will record at the introduction of this policy when the policy was last revised.

8. How to contact us

Questions regarding this policy, complaints about our practices and access requests should be directed to the *(insert company name)* Privacy Officer via e-mail at (*insert email address*) or by mail at *(insert mailing address).*

We will investigate all complaints and attempt to resolve those that we find are justified. If necessary, we will amend our policies and procedures to ensure that other individuals do not experience the same problem.

(Note to researchers: If your firm participates in TRUSTe's privacy program or another third-party privacy credentialing service, then mention that fact here. TRUSTe, for example, provides a dispute resolution service which they require their members to include in their privacy policies.)

ESOMAR
Eurocenter 2
Barbara Strozzilaan 384
1083 HN Amsterdam
The Netherlands
Tel +31 20 664 2141
Fax: +31 20 664 2922
E-mail professional.standards@esomar.org
www.esomar.org

ESOMAR is the world organisation for encouraging, advancing and elevating market research worldwide.