ESOMAR
WORLD RESEARCH

Revised 6 June 2017

World Research Codes and Guidelines

# ESOMAR DATA PROTECTION CHECKLIST

ESOMAR is the global voice of the data, research and insights community, speaking on behalf of over 4900 individual professionals and 500 companies who provide or commission data analytics and research in more than 130 countries, all of whom agree to uphold the ICC/ESOMAR International Code.

# CONTENTS

# 1 INTRODUCTION

Researchers working in a global context increasingly face a patchwork of national laws designed to ensure respect for individual privacy and protection of personal data. They have a responsibility to review and comply with not only the legal requirements in the country where they operate, but also the national data protection requirements in all countries where they conduct research and/or process data.

At the same time, the relentless expansion of new technologies into all aspects of our lives has not only increased the volume of personal data potentially available to researchers, but also introduced new types of personal data that must be protected.

One thing that has not changed is the need for researchers to protect the reputation of market, opinion, and social research and data analytics through practices that safeguard the rights of data subjects and maintain the confidence clients in research outcomes.

# 2 SCOPE

The purpose of this document is to provide researchers, especially those working in smaller organisations that might not have extensive resources or experience in data protection requirements, with general guidance on their responsibilities within a global data protection framework to ensure that data subjects retain control over their personal information. The specific framework used was developed by the Organisation for Economic Co-operation and Development (OECD). This framework includes a set of eight principles for use in designing programs to ensure privacy and protect personal data:

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness
- Individual participation
- Accountability

These broad principles are reflected in most existing and emerging privacy and data protection laws worldwide.

However, researchers should note that the OECD principles tie most closely to the EU's data protection requirements, and so researchers working in other regions are urged to consult other frameworks that may apply. They include the Asia-Pacific Co-operation (APEC) Privacy Framework, the EU-US Privacy Shield Framework, the Swiss-US Privacy Shield Framework, and the Generally Accepted Privacy Principles (GAPP) developed by the American Institute of CPAs (AICPA) and the Canadian Institute of Chartered Accountants (CICA). Although these frameworks generally do not have the force of law, they nonetheless express basic principles that researchers must adopt when working in the appropriate region.

In addition, researchers must review and comply with the national data protection and market research self-regulatory requirements of each country where they plan to do fieldwork 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 full compliance. They also may find it helpful to consult The Data Protection Laws of the World, an online resource hosted by DLA Piper that is updated annually.

Finally, researchers doing research in specialised areas such as healthcare research may wish to consult specific guidance such as the EphMRA Adverse Event Reporting Guidelines 2014 for further guidance.

## 3 USE OF "MUST" AND "SHOULD"

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.

## 4 DEFINITIONS

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

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

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

***Data analytics*** means the process of examining data sets to uncover hidden patterns, unknown correlations, trends, preferences, and other useful information for research purposes

***Data controller*** means a person or organisation responsible for determining how personal data is processed. For example, a research client would be the controller of data on its clients or customers; a government welfare agency would be the data controller for data collected from its welfare recipients; 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.

***Data subject*** means any individual whose personal data is used in research.

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

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

***Non-research activity*** means taking direct action toward an individual whose personal data was collected or analysed with the intent to change the attitudes, opinions or actions of that individual.

***Passive data collection*** means the collection of personal data by observing, measuring or recording an individual's actions or behaviour.

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

***Primary data*** means data collected by a researcher from or about an individual for the purpose of research.

***Privacy notice*** (sometimes referred to as privacy policy) means a published summary of an organisation's privacy practices describing the ways an organisation gathers, uses, discloses and manages a data subject's personal data.

***Processing of personal data*** includes, but is not limited to, their collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, whether by automated means or otherwise.

***Research*****,** which includes all forms of market, opinion, and social research and data analytics, means the systematic gathering and interpretation of information about individuals and organisations. It uses the statistical and analytical methods and techniques of the applied social, behavioural and data sciences to generate insights and support decision-making by providers of goods and services, governments, non-profit organisations and the general public***.***

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

***Research client or data user*** means any individual or organisation that requests, commissions, sponsors or subscribes to all or any part of a research project.

***Secondary data*** means data collected for another purpose and subsequently used in research.

***Sensitive data*** means specific types of personal information that local laws require be protected at the highest possible standards from unauthorized access to safeguard the privacy or security of an individual or organization and which may require additional explicit permission from the data subject to process. The designation of sensitive data varies by jurisdiction and can include a data subject's racial or ethnic origin, health records, sexual orientation or sexual habits, criminal records, political opinions, trade association membership, religious or philosophical beliefs, location, financial information, and illegal behaviours such as regulated drugs or alcohol..

***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.

***Trans-border 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 and use of cloud technologies for data.

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

## 5 SELF-HELP CHECKLIST ON DATA PROTECTION POLICY AND PROCEDURES

Users of the checklist below may note that the headings and order of items are not the same as those used by the OECD. The intent here is to express the principles in language and in an order that is more familiar to researchers. Readers also may recognise that the items are interrelated and sometimes overlapping. **Nonetheless, it is essential that the checklist be viewed as whole and individual items seen as complementary rather than exclusive, paying special attention to differences that depend on whether an organisation is acting as a data controller or a data processor. Any question for which the answer is not "yes" signals a potential gap in a privacy protection programme and therefore a potential risk of violating one or more data protection laws.**

## 5.1 Minimum impact

1. *When designing a research project, do you limit the collection of personal data, to only those items that are necessary to the research purpose and ensure they are not used in any manner incompatible with these purposes?*

Researchers must only collect, acquire, and/or hold personal data necessary from a quality control, sampling, and/or analytic perspective. In the case of B2B research, this includes personal data on data subject's position or level within a company, since that can be necessary to the purpose of the research.

This same principle applies to passive data collection methods as well as when working with secondary data sources. Therefore, it is the responsibility of the researcher to ensure that the only personal data items used in the research are those that are necessary to the research purpose. In the event that other personal data is received, those items must be filtered out and deleted.

2. *Do you implement processes that ensure that data subjects are not harmed or adversely affected as the direct result of their personal data being used in a market research project?*

Researchers must ensure that personal data cannot be traced nor an individual data subject'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 employee in a customer satisfaction survey.

3. *If you plan to use subcontractors or other third-party suppliers to perform services on your behalf, do you disclose the minimum amount of personal data that is necessary for them to perform the agreed upon services? Do you have contracts in place that ensure a similar level of protection on their part?*

When using a subcontractor, only provide the minimum amount of personal data required to perform the agreed-upon service, always making it clear via contracts and instructions the subcontractor's responsibilities while in the possession of those data. All sub-contractors must adhere to the same rules and regulations as the research organisation. Further, transferring of personal data to a subcontractor or other third party supplier must only be done with the prior consent of or commissioned by the research company's client.

The above assumes that that all data used in the research will remain confidential and will only be analysed and reported on at an aggregated level. If data subjects give their consent to link their responses to their personal data, then they must be informed how that information will be shared and used.

## 5.2 Notice and consent

4. *When doing primary data collection, do you obtain consent from every data subject whose personal data is to be collected?*

Under the OECD Privacy Principles any personal data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. Generally, national laws provide a number of lawful and fair grounds, but in most instances researchers will be obliged to rely on consent.

Consent must be:

- free (voluntary and able to be withdrawn at any time);
- specific (relating to one or more identified purposes); and
- informed (in full awareness of all relevant consequences of giving consent).

Consent must also be clearly indicated by a statement or action by the data subject having been provided with the information set out under items below. In summary, he or she should be informed about (a) the use to which his or her personal data will be put; (b) the specific data to be collected; (c) the name, address, and contact information of the company or organisation collecting the data and, if not the same organisation, the data controller; and (d) whether data will be disclosed to third parties.

Researchers should consider carefully the mechanism they use to obtain consent, usually expressed as opt out, opt in, implied, informed, or explicit. The specific method chosen should be documented.

In general, the more sensitive, intrusive, or non-obvious the data collection, the higher the standard of consent that is required. In some jurisdictions there are defined classes of "sensitive personal data" that require the explicit consent of the individuals concerned before they can be collected.

There can be instances in which researchers collect or receive personal data unintentionally or from persons not defined as data subjects of the research. Examples include information that is volunteered; client-supplied lists containing more information than is necessary to conduct the research; and bystanders captured in photographs or on video. Researchers should treat such information in the same manner as other personal data. Such data should be de-identified or destroyed immediately, particularly if there is no way of informing people whose data have been collected of its whereabouts, storage or usage. In some jurisdictions it is mandatory to delete such data or handle it in exactly the same manner as other information that has been captured intentionally.

*5. Are you clear about the purpose or purposes for which the data is collected and maintained?*

The research industry has long maintained a distinction between research and the collection of data for other purposes such as advertising, sales promotion, list development, direct marketing, and direct selling. This distinction is a critical ingredient in differentiating the purpose and promoting a positive image of research in the eyes of regulators and the general public. In recent years, the emergence of new technologies has increased the opportunities to collect personal information through techniques such as online tracking and downloadable mobile apps. In all cases it is essential that, prior to collecting any data, prospective data subjects are informed about the purpose(s) to which their data will be put and any potential consequences that may result including a follow up contact for quality purposes.

When researchers collect personal data from a data subject to be used for a market research purpose, transparency to the data subject is a critical element of the notice. The data subject must be given sufficient information about the intended use of the personal data collected and any sharing with third parties. By way of example, if the intended use of the personal data is to link a survey response to a customer profile that should be disclosed to the data subject at the time the personal data is collected.

Privacy notices must be reviewed on a regular basis to ensure that the type of data collected and the intended uses have not changed, and researchers must ensure that the actual business practices and technologies being used within the research organisation are consistent with the commitments made to data subjects and comply with evolving regulatory requirements. Each proposed use of personal data must be analysed to ensure compliance with local privacy laws, compliance with ICC/ESOMAR Code on Market, Opinion, and Social Research and Data Analytics and ESOMAR/GRBN guidelines, and consistency with the privacy promises made to data subjects.

*6. Are you clear about the specific data to be collected?*

Given the broad definition of personal data in certain jurisdictions, consider all of the possible personal data elements that may be collected when preparing data subject notices. Personal data may include name, address, email address, telephone number, mobile number, birthdate, mobile device identifier, IP address, photographs, audio and video recordings, national identifier

numbers (driver's license, social security, national insurance), user identifier assigned by your organisation, social media user name, data stored within a cookie or tracking pixel/tag. Remember also, a single data item by itself may not be deemed personally identifiable under local law, but when combined with other data (for example, zip code/postal code, gender, workplace or school, position and salary), may allow an individual to be singled out.

In addition, consider all of the possible recipients of the personal data. Researchers, research agencies, third-party service providers, and/or end clients all may have the ability to collect and/or use personal data in the course of a research project.

7. *Do you make clear how the data will be collected, including any passive data collection of which the data subject may not be aware?*

Historically, research has relied on interviewing as the primary method for collecting personal data. As noted in 5 above, new technologies have made it possible to collect a broader range of personal data without the knowledge of the individuals whose data is collected. All data subjects must be informed about the specific data being collected and the method(s) used to collect it, whether by an active means such as interviewing or a passive means such as via a mobile app or tracking behaviour via online cookies.

Researchers should consider which elements of the data collected and/or data collection method might be unanticipated to a data subject and provide prominent disclosure regarding such methods of collection. Consider "short form" notices layered over a more detailed privacy notice to describe data collection or use that might be unexpected or invasive. Mobile applications, particularly those that engage in geo location, "passive listening," and/or metering of the mobile device operating system, all require a detailed description and explicit consent from the data subject to such activities.

8. *When using personal data collected for some purpose other than research (e.g. customer data, social media data, etc.) do you ensure that the use is legitimate and the rights of data subjects are protected?*

Researchers and non-researchers alike increasingly look to acquire and use secondary data to augment or replace primary data collection. Prior to accessing and processing such data, researchers must ensure that their planned use is compatible with the purpose for which the data was originally collected. They must verify that the original collection was legal and with the consent of the data subjects, expressed or implied. In addition, they must establish legitimate interest by ensuring that the purpose is solely for research.

Researchers also must design their research so that further processing of the data does not risk causing harm to data subjects. Researchers must put safeguards in place to mitigate the risk of such harm such as ensuring that the identify of individual data subjects is not disclosed or revealed without prior consent, with measures to reduce the granularity of the data and lower the probability of an individual being singled out, and ensuring no non-research activity will be directed at them as a direct consequence of their data having been used for research.

## 5.3 Integrity/Security

9. *Are procedures in place to ensure that all personal data is accurate, complete, and up-to-date?*

Quality checks should be performed at every stage of the research process. When developing questionnaires or research applications, testing should be conducted before fieldwork begins to minimise the risk of errors in data collection. During the fieldwork stage, monitoring and validating interviews should be undertaken in accordance with applicable research quality standards. During the data processing and reporting stages, additional quality checks should be performed to ensure that the data is correct and that the analysis, conclusions, and recommendations are consistent with the data.

Researchers operating panels should ensure that panel members are able to review and update their profile data at any time and they should be reminded periodically to do so. Samples drawn from panels should include up to date demographic information. A good source for standard practices in this regard is ISO 26362:2009 – Access panels in market, opinion, and social research.

When using secondary data, researchers should review the quality checks employed at the time of collection to ensure that the data is accurate.

10. *Do you ensure the personal data is preserved no longer than is required for the purpose for which the information was collected, acquired, or further processed? Do you have procedures to separately store or remove identifiers from data records once they are no longer needed?*

Researchers should set data retention periods that are as short as possible, but in any event based on applicable laws, the source of the personal data they collect, and whether they are acting as data controllers or data processors. In the latter case, clients may impose retention periods by contract.

Regarding the source of personal data, information from longitudinal studies or profile information about panellists will typically be used and retained throughout the entire time that they remain active members. By contrast, a much shorter retention period should apply to personal data about non-panel data subjects who participate in ad hoc research. Obviously, it is important not to destroy their personal data too quickly since quality checks must be performed during the data processing stage to ensure accuracy and satisfy the requirements of the data integrity privacy principle.

When personal data is used, it is best practice for researchers to use pseudonymous identifiers. A master file linking data subjects' names, addresses or phone numbers with their corresponding internally-generated ID numbers must be kept secure with access limited to a small number, e.g. sampling or panel management staff. Thus, researchers, data processing, or coding staff who have a business need to analyse individual-level data can do so without seeing data subjects' names, addresses or phone numbers.

When survey responses have been processed and reported as aggregated, statistical data, personal data of data subjects, together with their corresponding pseudonymous identifiers, should be deleted, so that the research organisation no longer holds personal data.

11. *Are there procedures in place for responding to requests from data subjects about personal data you may have from him or her? Do your procedures for handling access requests from data subjects include authenticating their identities, responding to their requests in a reasonable period of time, allowing them to correct inaccurate data or deleting the data entirely?*

Formal procedures should be developed, communicated, and followed to respond to daa subjects who wish to access personal data that organisations hold about them. Authenticating the identities of data subjects who make access requests is important to prevent disclosing personal data to others inappropriately.

Once the identity of a data subject making an access request has been authenticated – the person is who he or she claims to be and has a legal right to access the personal data in question – researchers should endeavour to fulfil the access request as quickly as possible, e.g. within 10 to 30 days depending on applicable laws. If the research firm requires additional time to fulfil the request, it may be able to extend the deadline set out in law, provided that the individual is notified and the reasons for extending the deadline are sound. Additional time may be necessary, for example, to conduct consultations or to gather the requested information from multiple databases and sources.

Whilst data protection laws may include exemptions that require organisations to refuse a data subject access to personal information in certain situations, those exemptions are unlikely to apply to personal data being processed for a research purpose. For example, applicable laws may allow organisations to deny access requests if the information falls under solicitor-client privilege. By way of another example, if the organisation has disclosed information to a

government institution for law enforcement or national security reasons, that institution may instruct the organisation to refuse access or not to reveal that the information has been released.

*12. Are there security protocols in place for each data set that protect against risks such as loss, unauthorised access, destruction, use, modification, or disclosure?*

Fulfilling these responsibilities starts with developing and implementing a security policy to protect personal information and other types of confidential information. ISO 27001 is a recognised information security standard upon which a thorough security policy can be based.

The use of appropriate security safeguards to provide necessary protection includes:

- physical measures (locked filing cabinets, restricting access to offices, alarm systems, security cameras)
- technological tools (passwords, encryption, firewalls)
- organisational controls (background checks, rules relating to taking computers off-site, limiting access on a "need-to-know" basis, staff training, agreements with clients and subcontractors)

The security policy should also include a procedure for dealing with a potential data breach in which personal data is disclosed. In the case of secondary data collected by another party, such as a client's database, that party must be informed immediately. Data subjects whose data was disclosed also must be notified if the disclosure exposes them to some risk (e.g. identity theft) and appropriate steps taken to protect against that risk.

*13. Is there a clear statement on how long personal data is retained?*

The length of time personal data is retained may vary from one research project to another depending on a variety of circumstances noted previously in the response to question 9.

Whilst general retention practices should be included in privacy notices, it may not always be practical to communicate precise retention timelines for different types of studies. Therefore, researchers should also consider communicating data retention information in study recruitment materials, questionnaire introductions or study-specific consent forms. They should always be prepared to communicate data retention timelines for a given project upon request.

## 5.4 Transfer of data

*14. Do you have defined rules and procedures governing the use and disclosure of personal data?*

These rules and procedures are clearly outlined in the local privacy and data protection laws that exist in your country. An explanation of what that means should be clearly documented with processes and written documents to ensure staff can implement the procedures on how to manage personal data and are familiar with these rules and procedures. For instance, this will include the principle that consent is required from the data subject before any such data can be disclosed, even to clients or researchers in client organisations and regardless of whether it was collected by the researcher or some other party.

*15. Are the conditions under which personal data may be disclosed clear and unambiguous?*

Data subjects must know what is happening with their personal data and this must be either explained verbally or provided in some written format or document that data subjects have agreed to – e.g. via their consent which is recorded as evidence that they have agreed.

*16. Are your staff aware of those rules and trained in how to implement the procedures?*

Your privacy policy describes your firm's data collection and management practices. It is equally important to develop internal standard operating procedures (SOPs) to ensure that the privacy promises made to data subjects are kept.

Staff training on privacy should include an overview of applicable laws, industry codes of conduct, your firm's consumer-facing privacy policies, and your SOPs. Privacy training should be delivered at least annually and attendance records should be kept.

All frontline staff who interact with data subjects should be able to explain their firm's policies and procedures at a high level. They should know whom to contact internally for assistance with inquiries that they are not able to answer.

There should be clear supervision and responsibility outlined including some form of monitoring that procedures are being followed.

## 5.5 Trans-border transfers of personal data

17. *If personal data is to be transferred from one jurisdiction to another, is it done in such a way that it meets the data protection requirements in both the origin and destination jurisdictions?*

This is often referred to as a "trans-border transfer of personal data". It occurs when data is collected across national borders and or when data processing is offshored or outsourced to another country (e.g.when a client engages a researcher in another country to carry out a study using client supplied customer or service user data). Each country has its own rules on how such data must be treated and protected which researchers must comply with. Whilst this may seem complex, it helps if the compliance issues faced by researchers are broken down into three main issues:

- Ensuring trans-border transfers of personal data is carried out in compliance with applicable international, and national laws, regulations and frameworks. The most common grounds to ensure adequate protection for a trans-border transfer will be either consent or the use of appropriate contractual clauses and, where required by applicable national law, obtaining prior authorisation from the national Data Protection Authority or other applicable privacy regulatory authority to the use of those contracts. As an additional security measure and to further reduce risk where data processing is offshored, identifying personal data should be removed where practicable so that only a pseudonymous ID number is used to link individual-level data with data subjects' identities.
- The extent to which a researcher may be able to carry out trans-border transfers when acting as a data processor, such as when carrying out a study using client supplied sample. Even where researchers have taken care to ensure any trans-border transfers comply with the rules governing such transfers, they should keep in mind that when processing personal data as a data processor acting on behalf of a data controller (e.g. the research client), they, as data controller may not be able to permit trans-border transfers of personal data they control, which may impact how they are able to carry out the project. There should be a written agreement in place between both parties on the above.
- Trans-border transfers of personal data involving personal data from subjects in other countries (e.g. online surveys aimed at data subjects resident in a different country(s) to that in which the researcher is controlling the study). The applicable privacy laws will normally be the national laws of the country where the researcher is based. However, the researcher must also ensure the study or panel is compliant with any other applicable national laws in countries were data is being collected. Recommended practices include ensuring that: (1) the researcher's legal details (company name, postal address etc.) including country is clearly communicated in all recruitment material; (2) the online privacy policy used includes a simple but clear statement outlining the trans-border transfers that will take place by participating in the study or panel; and (3) there is a reference to the trans-border transfer(s) within the panel recruitment consent question.

## 5.6 Out-sourcing and sub-contracting

*18. Are there clear requirements including appropriate oversight for any outside data processors or other subcontractors?*

There must be clear requirements communicated to all outside data processors or other subcontractors to follow required data protection rules relating to personal data when any form of data is transferred. There should be additional protection in the transfer of any data, be that at personal or aggregated level with the use of dedicated IT processes such as encryption of data in transfer or use of secure FTP transfer platforms. If copies are to be made of any data as backup by subcontractors or outside data processors, then there must be clear processes to protect that data during storage and to delete it when no longer required.

*19. Is there an agreement (contract) in place with all subcontractors used?*

There must be an agreement in place with any subcontractor that is engaged. The contract should address the business terms of the engagement (including statement of work, term, insurance, etc.) as well as the:

- data protection requirements; and
- Information security requirements.

## 5.7 Privacy notice

*20. Is information about your privacy and personal data protection programme readily available and in a form that is easily understood by participants?*

Many jurisdictions require that information be available in a privacy notice that is readily available to data subjects. Although the content and detail required varies from country to country, researchers must always identify themselves clearly to data subjects and ensure that they explain the purpose of the research, how personal data is collected, how it will be managed (collected, stored, used, accessed and disclosed), and how to obtain more information or lodge a complaint.

Researchers must ensure that policies are easy to understand, relevant to the reader, easy to locate, as concise as possible, and tailored to the organisation's operations. This includes making policies available in as many languages as practical, reviewing them regularly, and updating them as applicable.

*21. Is the identity and responsibility of the data controller clear?*

Researchers must ensure that their own roles and responsibilities for managing personal data is clear to data subjects. This includes identifying the data controller and whether any external data processors are being used. Data subjects must not be left in doubt as to which organisation is ultimately accountable for managing their data.

Some jurisdictions also require that a specific individual be identified as having responsibility for the company's data protection practices.

In the case of blinded surveys using client-supplied samples, participants should be told at the beginning of the interview that the client's name will not be revealed until the end of the survey because divulging this information up front could introduce a response bias. Since many national data protection laws give data subjects a legal right to know from whom the researcher obtained their personal data, researchers must be prepared to identify the client's name at any time upon request.

*22. Is it clear that the data controller is accountable for personal data under its control regardless of the location of the data?*

If researchers are likely to subcontract any of the processing, or transfer personal data outside their own jurisdiction, they should be prepared to provide the data controller with details of the subcontractors and locations of the processing; and obtain prior written consent from the data controller where necessary. Where the research agency is the data controller, they should include

references to use of data processors and, where relevant, list the countries or broad regions in their privacy policies. Researchers should be alert to the fact that some jurisdictions prohibit researchers from transferring personal data to countries or regions that do not have equivalent levels of data protection law. Subject to compliance with the rules governing trans-border transfers imposed by relevant local national law, transferring personal information across a multi-national group is allowed by most jurisdictions, although some still require data subjects to be notified of the locations where data may reside.

# 6 SPECIAL ISSUES

## 6.1 Collection of data from children, young people, and other vulnerable individuals.

Researchers must obtain the consent of the parent or responsible adult before collecting personal data from any data subject for whom a legal guardian has been appointed. When asking for consent, the researcher must provide sufficient information about the nature of the research project to enable the parent or responsible adult to make an informed decision about the data subject'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 data subject;
- an explanation of how the data will be protected and used;
- an explanation of the reasons the data subject 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 data subject.

There currently is no common international definition of a child or young person. Even within a single country the definition can vary. Settling on an alternate definition based on characteristics other than age (e.g. cognitive abilities) and then applying it in a research setting is difficult if not impossible. Therefore, researchers must rely on any relevant definitions expressed in applicable local laws, codes of conduct, and cultural norms. In the absence of clear guidance ESOMAR and GRBN recommend defining a child as being 12 and under and a young person as aged 13 to 17. For further details, consult the ESOMAR guideline, Interviewing Children and Young People.

## 6.2 Business-to-business research

A substantial number of research projects involve collection of data from legal entities such as businesses, schools, non-profits, and similar organisations. 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).

## 6.3 Photographs, audio, and video recordings

A number of new research techniques create, store, and transmit photographs, audio, and video recordings as part of the research process. Two prominent examples are ethnography and mystery shopping.

Researchers must recognise that photographs, audio, and video recordings are personal data and must be handled as such. If researchers ask data subjects to provide information in these forms, they also should provide guidance on how to reduce collection of unsolicited data, especially from non-participants.

Finally, some types of observational research may involve photographing, videoing or recording in public settings involving people who have not been recruited as data subjects. In such instances, researchers must gain permission to share such images from those data subjects whose faces are clearly visible and can be identified. If permission cannot be obtained, then the data subject's image should be pixelated or otherwise anonymised. In addition, clear and legible signs should be placed to indicate that the area is under observation along with contact details for the individual or organisation responsible. Cameras should be sited so that they monitor only the areas intended for observation.

## 6.4 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. Many cloud storage service providers offer weak indemnities in the event that they cause security breaches and personal data is 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 data subjects.

Researchers should therefore implement compensating controls to protect against such risks. For example, they should encrypt personal data while in motion (transferred to/from the cloud) and at rest (stored on the cloud provider's servers). Researchers also should consider purchasing a cyber-liability insurance policy.

Researchers also must consider the physical locations at which personal data is stored to determine whether use of cloud storage is a trans-border transfer. Refer to Section 5.5 of this document for further discussion. Some cloud service providers offer country-specific storage locations that may be appropriate in some instances.

Finally, researchers should locate personal data on a private cloud, rather than a public one. A private cloud is one in which dedicated equipment in a particular data centre is assigned to the researcher's firm. The main benefit of a private cloud is that the researcher always knows where the personal data is located. By contrast, a public cloud may result in data being located in two or more data centres and two or more 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.

## 6.5 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 or modification 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 to ensure they will not make it 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 by using a unique identifier such as an ID number, or hashing algorithms, whilst holding their personal data separately for checking purposes (see Q9).

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 SOURCES AND REFERENCES

DLA Piper, Data Protection Laws of the World

EphMRA Adverse Event Reporting Guidelines 2014

ICC/ESOMAR International Code on Market and Social Research

ESOMAR Interviewing Children and Young People Guideline

ISO 26362:2009 – Access panels in market, opinion, and social research

Privacy Shield Framework

OECD Privacy Principles

## 8 THE PROJECT TEAM

Co-Chairs:

- Reg Baker, Consultant to the ESOMAR Professional Standards Committee and Marketing Research Institute International
- David Stark, Vice President, Integrity, Compliance and Privacy, GfK

Project Team members:

- Debrah Harding, Chief Operating Officer, Market Research Society
- Stephen Jenke, Consultant
- Kathy Joe, Director of International Standards and Public Affairs, ESOMAR
- Wander Meijer, Global COO, MRops
- Ashlin Quirk, General Counsel at SSI
- Barry Ryan, Manager, Global Privacy - Program, Policy & Governance, American Express
- Jayne Van Souwe, Principal, Wallis Consulting Group