ESOMAR

Data Protection Checklist

To help you identify key areas that need attention when designing research projects

ESOMAR champions the research, insights, and analytics sector worldwide. Founded in 1947, the global membership association is a network reaching over 50,000 professionals and 750+ companies in 130+ countries. We support our global community through raising ethical standards, facilitating education, advocating with legislators, sharing best practices, promoting evidence-based solutions for decision-makers, and ensuring the values of honesty, transparency, and objectivity are applied to all data sources.

The purpose of this Checklist is to provide researchers and organisations with general guidance on their responsibilities within a global data protection framework to ensure that data subjects retain control over their personal information. It will be especially helpful to those that might not have extensive resources or experience in data privacy compliance, to identify the key issues that need to be taken into account when designing research projects.

Published by ESOMAR Amsterdam, The Netherlands

ISBN number : 92-831-0323-8

Volume S411

Any question for which the answer is not "yes" signals a potential gap in a privacy protection programme and a potential risk of violating one or more data protection laws thus indicating that additional protections need to be incorporated.

1. *When designing a research project, do you limit the collection of personal data to only those items that are adequate, relevant and necessary in relation to the purpose for which they are processed and do you ensure that they are not used in any manner that is incompatible with such purpose?*

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

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?*

4. *If you plan to collect data from children, young people or other vulnerable persons, do you obtain the consent of the parent or Responsible Adult before collection?*

5. *Can you identify a lawful basis for processing the personal data?*

6. *Are you processing personal data only for their intended use?*

7. *Do you make it clear about the specific data to be collected and maintained, including any passive data collection of which the data subject may not be aware?*

8. *When using secondary 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?*

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

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

11. *Is there a clear statement on how long personal data are retained?*

12. *Are there procedures in place to allow data subjects to exercise their rights as provided by the applicable laws and regulations?*

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

14. ***In case of a breach, can you provide affected data subjects with a description of the nature of the breach and the likely consequences?***

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

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

17. ***Is your staff aware of your organisation's policies and procedures and trained in how to implement them?***

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

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

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

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

22. ***Does your project utilise cloud-based infrastructure?***

23. ***Do you safeguard the identity of the participants before storing or sharing the data related to the project?***

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

This Data Protection Checklist is an integral part of a collection of guidance published by ESOMAR in the field of data protection, the ESOMAR/GRBN Guideline on duty of care, aimed at protecting research data subjects from harm; the ESOMAR/GRBN Guideline for researchers and clients involved in primary data collection; the ESOMAR/GRBN Guideline on reuse of secondary data, and the ESOMAR/GRBN Guideline of research and data analytics with children, young people, and other vulnerable individuals. Moreover, the specific framework used for this checklist was developed by the Organisation for Economic Co-operation and Development (OECD), which includes a set of eight principles for use in designing programmes to ensure privacy and protect personal data:

1. ***Collection limitation***
2. ***Data quality***
3. ***Purpose specification***
4. ***Use limitation***
5. ***Security safeguards***
6. ***Openness***
7. ***Individual participation***
8. ***Accountability***

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

Researchers and organisations should note that the OECD principles tie most closely to the EU's data protection requirements, and so organisations working in other regions are urged to consult other frameworks that may apply. At the time of this second edition of the Data Protection Checklist, they include the General Data Protection Regulation 2016/679 (EU), the Asia-Pacific Co-operation (APEC) Privacy Framework, the California Consumer Privacy Act (CCPA), the Canadian Personal Information Protection And Electronic Documents Act (PIPEDA) the European

Commission adequacy decisions, and the Generally Accepted Privacy Principles (GAPP) developed by the American Institute of CPAs (AICPA) and the Canadian Institute of Chartered Accountants (CICA). Although some of these frameworks do not have the force of law, they nonetheless express basic principles that organisations must adopt when working in the appropriate region.

As stated, researchers and organisations 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 jurisdiction. 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. Organisations may find it necessary to consult with 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, organisations doing research in specialised areas such as healthcare research may wish to consult further specific guidance such as the EphMRA Adverse Event Guidelines 2022.

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.

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

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

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

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

Data controller means a person or organisation responsible for determining how personal data are processed. For example, a research client would be the controller of data about 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 natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. A research company may be both data controller and processor for an omnibus study.

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

Deductive disclosure means the inference of a data subject's identity via cross-analysis, small samples or through combination with other data (such as a client's records or secondary data in the public domain).

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 data by observing, measuring or recording an individual's actions.

Personal data 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 a data subject for the purpose of research.

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

Privacy impact assessment means a process to identify and mitigate data subjects' privacy risks.

Privacy notice (sometimes referred to as a 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.

Responsible Adult means a person who has personal accountability for the well-being of a child, young person, or vulnerable individual including parents, legal guardians, and others responsible for day-to-day care. The parameters of the definition for responsible adult vary from country to country and as such national Codes and/or laws must be followed where such rules exist

Secondary data means data that has already been collected and is available from another source.

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

Terms of Use (also referred to as Terms of Service) means the policy, for example, for a website or online service, that requires its users and third parties to accept as a condition of using the service.

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 transfer of personal data means the movement of personal data across national borders by any means, including access of data from outside the jurisdiction where it is collected and the use of cloud technologies for data.

Vulnerable individuals refers to 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

Readers of this Checklist 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 organisations. 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 are seen as complementary, 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 a potential risk of violating one or more data protection laws.

5.1 Privacy by design and data protection impact assessment

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

Researchers must only collect, acquire, and/or hold personal data that are necessary from a quality control, sampling, legal, and/or analytic perspective. In the case of B2B research, this can include personal data on a data subject's position or level within a company, if those data are necessary for the purpose of the research.

This same principle also applies to passive data collection methods when working with secondary data sources. Therefore, it is your responsibility to ensure that only personal data items used in the research are those that are necessary for the research purpose and if other personal data are received, they must be filtered out and deleted.

Once collected you should conduct information audits to map data flows within your organisation. A data map is an important tool that identifies the flow of personal data which your process and their lifecycle within your organisation.

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

You must ensure that personal data cannot be traced, and that individuals cannot re-identified or have their 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 (or re-identify) an individual in a customer satisfaction survey. To establish the right level of security, you will need to also consider the personal data that you process and assess the risk of processing those data in combination with any additional information. For example, you should consider how sensitive or confidential a given category of data is or what harm could be caused to data subjects in case of unauthorised disclosure or security breach.

As part of a data protection by design approach, it is recommended that you conduct a privacy impact assessment (PIA or DPIA) to chart the planned flow of information through the project, to identify risks and assess their severity and likelihood. This is mandatory in most jurisdictions for any type of processing which is likely to result in a high risk to data subjects. All risks should be acted upon promptly to minimise them, and risk mitigation solutions must be integrated into organisational processes and plans.

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?**

There must be a written agreement between your organisation and the subcontractor, with clear instructions specifying the subcontractors' responsibilities whilst in possession of personal data. Such agreements must always include certain specific clauses, e.g. to delete and/or return all the personal data provided for the execution of the agreed upon service and only use the personal data for the agreed upon services. Agreements must always define minimum security standards. Indeed, you should only choose subcontractors who provide sufficient guarantees about their privacy, confidentiality and security measures and you should review such measures, for example, by requesting copies of prior security assessments.

Clear obligations must be communicated to all external data processors and other subcontractors to follow required data protection rules relating to personal data when data is transferred. Additional protection should be applied to the transfer of personal data or commercially sensitive data using dedicated IT processes such as encryption of data in transit (e.g. use of secure FTP transfer platforms) and at rest. There must be clear processes in place (both internally and externally) to protect that data during storage and to delete it when no longer required. This includes, for instance, situations where the data are processed by other third parties such as for hosting and backup purposes by cloud services providers.

To reduce any residual risk, only the minimum amount of personal data required to perform the agreed-upon service should be provided when using subcontractors who must adhere to the same rules and regulations as the research organisation. Onward transfer of personal data to a subcontractor or other third-party supplier must only be done with the prior written consent of the data controller.

The above assumes that all data used in the research will remain confidential and only analysed and reported to the end client at an aggregated or de-identified level. If an end client wishes to combine or link other data to the research results so that the data subjects could be identified, then those data subjects should give their consent for such processing and be informed how that information will be shared and used.

4. If you plan to collect data from children, young people or other vulnerable persons, do you obtain the consent of the parent or responsible adult before collection?

You must obtain the consent of the responsible adult before collecting personal data from any such data subject. When asking for consent, you must provide sufficient information about the nature of the research project to enable the guardian to make an informed decision about the data subject's participation, including as a minimum:

- *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 why the data subject has been asked to participate and the likely benefits or potential impacts;*
- *An outline of kinds of activities that might be undertaken (e.g. product testing) or any incentive being offered*
- *a description of the procedure for giving and verifying consent.*

You also should record the identity of the guardian and their relationship to the data subject. Once consent from the responsible guardian has been obtained, the researcher must also obtain the consent of the data subject before continuing.

There currently is no common international definition of a child or young person which can vary even within a single jurisdiction. As 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, you 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. (See the definition of children and the ESOMAR. GRBN Guideline on Research and Data Analytics with Children Young People and other Vulnerable People).

5.2 Lawful basis

5. Can you identify a lawful basis for processing the personal data?

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

Consent must be:

- Freely given (voluntary and able to be withdrawn at any time);
- Specific (relating to one or more clearly identified purposes); and
- Informed (in full awareness of all relevant consequences of giving consent);

While the **ESOMAR/GRBN Guideline for Researchers and Clients Involved in Primary Data Collection** is better suited to guide researchers on how to comply with primary data collection, it is important to remember that valid consent should be clearly indicated by a statement or action by the data subject, having been provided with the information set out below.

In summary, unless provided otherwise by the relevant legislation, best practice is that data subjects should be informed about:

1. the use to which their personal data will be put;
2. the specific data to be collected;
3. the name, address, and contact information of the company or organisation collecting the data and, if not the same organisation, the data controller, and;
4. whether data will be disclosed to third parties, unless otherwise provided by the applicable law.

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 collect.

There can be instances in which you 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 for instance in photographs, video or audio recordings. You

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.

However, consent is not the only lawful basis you can rely upon. Depending on the jurisdiction, there may be other lawful bases for processing:

Contract: the processing is necessary for a contract with the individual.
Legal obligation: the processing is necessary to comply with the law (this does not include contractual obligations).
Vital interests: the processing is necessary to protect someone's life.
Public interest: the processing is necessary to perform a task in the public interest or for an official function, and the task or function has a clear basis in law.
Legitimate interests: the processing might be necessary for your legitimate interests or the legitimate interests of a third party, providing that the personal data are being used in a manner that data subjects would reasonably expect, and the processing is unlikely to have a significant impact on their privacy.
Compatible purpose: where the new purpose is similar to the original purpose. In some jurisdictions, statistical research might be considered a compatible purpose. In such cases, you must observe the privacy protection safeguards described in this document.

No single basis is better or more important than another and you will need to research which is the most appropriate one, based on the purpose for processing and your relationship with the data subject. However most lawful bases require that the processing is necessary and for a specific purpose.

It is recommended to document which legal basis you rely upon, and to specify the reasons why you have relied upon that specific basis.

6. Are you processing personal data only for their intended use?

The research industry has long maintained a distinction between research and the collection of data for non-research 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.

Activities offered under the research umbrella must be limited to statistical/social science and behavioural analysis and delivery of insights that result in no direct action to an individual

Organisations must ensure that their employees are able to distinguish between research practices and other data collection and processing activities that have a non-research purpose, including taking direct action toward individual data subjects. For further guidance, consult the ESOMAR GRBN Duty of Care Guideline.

7. Do you make it clear about the specific data to be collected and maintained, 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. 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.

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. Remember that 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.

When researchers collect personal data from a data subject to be used for a market research purpose, transparency to the data subject is critical. The data subject must be given sufficient information about the intended use of the personal data collected, any sharing with third parties and any potential consequences that may result including a follow up contact for quality purposes. (see 5.5 Privacy notice).

You 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 secondary 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.

In line with the ESOMAR/GRBN Guideline on Use of Secondary Data, researchers must only use secondary data sources containing or constituting personal data that are adequately supported by information that specifies how the data was collected, under what terms, and for what purpose. Above all else, researchers must verify that the personal data was collected legally and transparently, which is essential when determining whether the data can be processed for a research purpose. You must obtain documentation to demonstrate confirmation on the ability and lawfulness to sell or share the data and for you to use the data.

You also must design your research so that further processing of the data does not risk causing harm to data subjects and is compatible with any statements made to data subjects such as Terms of Use when using a platform or signing up for a service. You must put safeguards in place to mitigate the risk of harm such as ensuring that the identity of individual data subjects is not disclosed or revealed without prior consent. These include 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.

6. Integrity and security

9. **Are procedures in place to ensure that all personal data are 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 are 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, for instance, ISO 20252:2019 "Market, opinion and social research, including insights and data analytics — Vocabulary and service requirements". When employing subcontractors, the security standards and practices above must cascade down to all actors involved in the value chain.

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

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

If identifiable personal data is shared with clients, you must outline the data retention policy. This includes entering legally binding agreements with those clients regulating the data retention periods to ensure that personal data are kept in a form that permits identification of the data subject for no longer than is necessary for the purpose for which they were processed, and in compliance with applicable laws.

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 a

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

When survey responses have been processed and reported, the personal data of data subjects, together with their corresponding pseudonymous identifiers, should be deleted, so that you no longer hold personal data. To do so, you should develop and follow internal policies that will enable staff to address residual security risks in a consistent manner. Such policy should clearly define the organisational approach to security together with roles and responsibilities for implementing it and monitoring its compliance.

11. Is there a clear statement on how long personal data are retained?

You should set data retention periods to ensure that personal data that can identify or re-identify an individual are kept for no longer than is necessary and only used for the purposes for which they were collected. The length of time personal data are retained may vary from one research project to another and in accordance with the applicable laws and regulations depending on a variety of circumstances noted previously in the response to question 10.

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, you should also consider communicating data retention information in study recruitment materials, questionnaire introductions or study-specific consent forms. You should always be prepared to communicate these timelines for a given project upon request and ensure that any data retention periods that have been agreed with a client are not in conflict with those communicated to data subjects.

12. Are there procedures in place to allow data subjects to exercise their rights as provided by the applicable laws and regulations?

Some jurisdictions provide for a data subject's right to access, erase, restrict the processing and request portability of their personal data. Your procedures for handling such access requests from data subjects should include authenticating their identities, responding to their requests in a reasonable period, and allowing them to correct inaccurate data and deleting the data.

Formal procedures should be developed, documented, communicated to the relevant stakeholders and implemented to respond to data subjects who wish to exercise their rights. In authenticating the identities of data subjects who make access requests, it is important to prevent disclosing personal data to others inappropriately. You should request the least intrusive information, e.g. if requesting a copy of their identity card, you can ask the requestor to conceal other non-relevant information on the document such as address, social security number, etc. You should pay careful attention to the time limits to respond to data subject requests imposed by applicable law.

Once the identity of a data subject making an access request has been authenticated, you should endeavour to fulfil the request as quickly as possible, but in any event, within 30 days subject to any stricter applicable laws (e.g. under the Brazil LGDP, the time limit is 14 days). If the research organisation 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 gather the requested information from multiple databases and sources.

Data protection laws may include exemptions that require organisations to refuse a data subject access to personal information in certain situations, and it is important that researchers are aware of them. For example, applicable laws may allow organisations to deny access requests if the organisation has disclosed information to a government institution for law enforcement or national security reasons. Equally, disclosure might result in another data subject's personal data being revealed.

Some jurisdictions provide for an exemption from the right of access if personal data is processed for scientific or historical research or statistical purposes. Researchers are advised to check if the

required conditions for an exemption are fulfilled such as measures to minimise data, ensuring that the research results are not made available in any way that identifies individuals and that the processing is not likely to cause an impact, substantial damage or distress to an individual.

13. 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, virtual private network)
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, together with regular audits or protocols and technology to ensure information security standards are met)

Organisations might be required to appoint a person or department in charge of developing, implementing and monitoring the security policy (Data Protection Officer under GDPR) who is to be given the necessary authority and resources.

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

If you use a data processor (or sub processor), the requirements on breach reporting should be detailed in the contract between you and the data processor (or sub processor).

The data controller must report a notifiable breach to the data protection authority with jurisdiction without undue delay. Under the GDPR, this is specified as being no later than 72 hours

after becoming aware of the breach and if you take longer than this, you must give reasons for the delay. However, you should ensure you are fully aware of the time limits imposed by local applicable law.

14. When reporting a data breach, you must provide a description of the nature of the breach including, where possible:

- the categories and approximate number of individuals concerned;
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

6.1 Use of data

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

These rules and procedures are often specified in the local privacy and data protection laws of the applicable jurisdiction. An explanation of what that means should be clearly documented with processes and procedures to ensure staff can implement those processes and procedures, understand how to manage personal data and are familiar with them. 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. Further, it is essential that you obtain from clients a written guarantee that the client will not attempt to re-identify data subjects including reverse engineering or de-identification techniques unless the data subject has given explicit consent that their identifiable information can be shared with the client, and the purpose is for research only.

16. 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.

17. Is your staff aware of your organisation's policies and procedures and trained in how to implement them?

Your privacy notice describes your firm's data collection and management practices. It is important to develop and document 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 data subject-facing privacy notices, 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 enquiries 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.

18. If personal data is to be transferred from one jurisdiction to another, or if data is collected across borders, is it done in such a way that it meets the data protection requirements in both the origin and destination jurisdictions?

Each jurisdiction has its own rules on how 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 cross-border transfer of personal data is carried out in compliance with applicable international, and national laws, regulations and frameworks where they exist. The most common grounds to ensure adequate protection for a cross-border transfer will either be consent or the use of appropriate contractual clauses and in compliance with the applicable laws, obtaining prior authorisation from the national Data Protection Authority or other applicable regulatory authority, to use 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 cross-border transfer 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 cross-border transfer 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), the client as data controller may not permit cross-border transfer of personal data. This may impact how the researcher will be able to carry out the project. There should be a written agreement in place between both parties on the above, including notifying the client in advance of any such transfer.*
- *Processing of personal data outside the country of origin (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 laws of the jurisdiction where the researcher is based. However, the researcher must also ensure the study or panel is compliant with any other applicable laws of the relevant jurisdiction where data are 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 cross-border data collection that will take place by participating in the study or panel; and (3) there is a reference to the cross-border collection(s) within the panel recruitment consent question.*

You must be aware that data localisation, also known as data residency, is a legal requirement applicable in certain jurisdictions providing that data on a country's citizens or residents be collected, processed, and/or stored within the country before they may be transferred across borders.

6.2 Privacy notice

19. 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 between jurisdictions, you must always identify yourself clearly to data subjects and ensure that you explain the purpose of the research, how personal data are collected, how it will be managed (collected, stored, used,

accessed, transferred and/or disclosed), and how to obtain more information or lodge a complaint.

You 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.

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 you 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 the applicable privacy laws and regulations, compliance with ICC/ESOMAR International Code on Market, Opinion, and Social Research and Data Analytics and ESOMAR/GRBN guidelines, and consistency with the privacy promises made to data subjects.

20. Is the identity and responsibility of the data controller clear?

Researchers must ensure that their own roles and responsibilities for managing personal data are made 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. For example, when the end client provides the research agency with an existing panel of respondents, the client determines the processing purpose and the way in which data processing is to be approached and is thus the data controller.

Some jurisdictions also require that a specific actor in a data chain can be identified as data controller or as having responsibility for the company's data protection practices regardless of their actual involvement in data collection and processing to ensure it is clear who is accountable for determining the purposes and means of the processing of personal data.

In the case of blinded surveys, 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. Researchers should check whether under the applicable data protection law, data subjects have a legal right to know from whom the researcher obtained their personal data at any time upon request and who is the data controller.

Subject ot the rules governing data privacy in that jurisdiction, when receiving the name of the client, the participant should be given the opportunity to opt out of the survey.

21. Is it clear that the data controller is accountable for personal data under their 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 notify the client in advance of any such transfer where necessary. Where you are the data controller, you should include references to use of data processors and, where relevant, list the countries or broad regions in your privacy policies. You 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. Most jurisdictions treat transferring personal information across a multi-national group the same way as between unconnected parties. It is therefore best to assume that they require full compliance with the rules governing cross-border transfer imposed by relevant local law.

6.3 Cloud storage

22. Does your project utilise cloud-based infrastructure?

Researchers must assess the cloud storage service provider's security controls and its standard terms and conditions including for security breaches where personal data are compromised.

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

You also must consider the (a) physical locations at which personal data are stored to determine whether use of cloud storage is a cross-border transfer and (b) from where they might be accessed or accessible (whether just for database maintenance or not), as even such possibility constitutes a cross-border transfer. Some cloud service providers offer country-specific storage locations that may be appropriate in some instances.

Finally, you 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 you and has the main benefit that you always know where the personal data is located. By contrast, a public cloud may result in data being located in two or more data centres and even continents, raising possible compliance issues, both with applicable requirements under data protection laws and with contracts with data controllers, which specify where personal data must be located.

6.4 De-identification and pseudonymisation

23. Do you safeguard the identity of the participants before storing or sharing the data related to the project?

A key part of your data protection responsibility is to de-identify data as far as possible during storage or prior to release to a client or even the general public. De-identification 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 identifying personal data separately.

When employing such techniques, you should consult relevant jurisdictions 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

- ICC/ESOMAR International Code on Market and Social Research and Data Analytics
- ESOMAR/GRBN Guideline on duty of care,
- ESOMAR/GRBN Guideline for researchers and clients involved in primary data collection;
- ESOMAR/GRBN Guideline on reuse of secondary data,
- ESOMAR/GRBN Guideline of research and data analytics with children, young people, and other vulnerable individuals.
- OECD Privacy Principles
- ISO 20252:2019 "Market, opinion and social research, including insights and data analytics

- ISO/IEC 27001 and related standards Information security management
- EphMRA Adverse Event Guidelines 2022
- DLA Piper, The Data Protection Laws of the World

8 The Project Team and Contributors

- Judith Passingham, Chair of ESOMAR's Professional Standards Committee
- Kim Smouter, Chair of ESOMAR's Legal Affairs Committee
- Kathy Joe, Consultant to ESOMAR's Professional Standards Committee
- Prof. Dr. Raimund Wildner, Managing Director and Vice-President at GfK Verein
- Philippe Guilbert, Consultant to Syntec Conseil
- Reg Baker, Former Consultant to ESOMAR's Professional Standards Committee
- Rupert van Hüllen, Global Chief Privacy Officer at Ipsos
- Ravinder Roopra, Group Global Head of Privacy and Data Protection Officer at Kantar