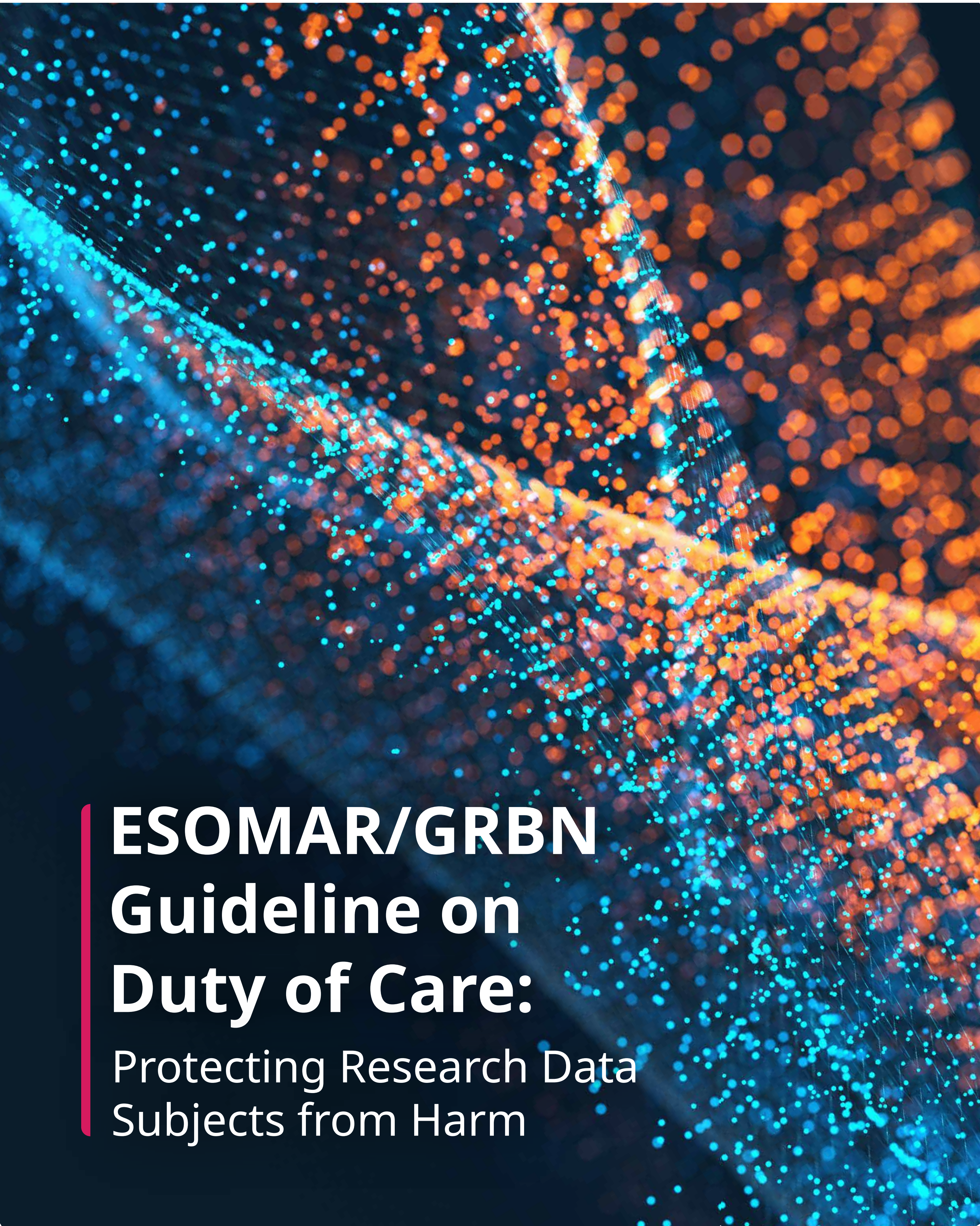
ESOMAR

GLOBAL RESEARCH BUSINESS NETWORK
APRC • EFAMRO • ARIA • AMRA



ESOMAR/GRBN Guideline on Duty of Care:

Protecting Research Data Subjects from Harm

Contents

1 Introduction

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

Historically, researchers' primary ethical responsibility has been to protect data subjects from harms such as unsolicited direct marketing and other similar sales-oriented activities. More recently, the proliferation of data of all kinds and the ability to link data from multiple sources to create rich profiles on individual data subjects has led to new uses of data that go beyond marketing and sales to a host of other domains such as the provision of healthcare services, granting of credit, criminal justice investigations, and employment decisions, to name a few. Such uses not only compromise the privacy of data subjects, they also can be discriminatory, favouring some individuals over others and potentially doing so based on incomplete or biased information.

At the same time, the continually expanding use of modern technologies for data acquisition, processing, analysis and delivery by organisations in all sectors has created a new set of risks for data subjects. They include the unauthorised release of personal data or data breaches by outside persons or organisations.

Meeting our profession's responsibility to protect the privacy and well-being of data subjects requires that organisations and individuals that commission or conduct research provide an adequate and effective infrastructure of processes, tools, standards and technologies for protecting any personal data in their possession from accidental or other unauthorised disclosure. They must recognise that they are ultimately accountable to data subjects and regulators should such disclosures occur.

2 Purpose And Scope

The purpose of this guideline is to advise researchers and those who do research on behalf of clients about their responsibility to protect the privacy and well-being of data subjects who participate in research or whose data is processed for a research purpose. It is also designed to provide guidance for those who commission research to ensure that they are fully aware of their responsibilities and to set expectations about what is and is not possible given established ethical and legal requirements.

While this guideline is directed primarily at researchers, including those in client organisations and others focused primarily on data analytics, it also applies broadly to any individual or organisation involved in the collection and/or processing of personal data for research.

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

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

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

3 Definitions

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

API (application programming interface)

A set of definitions on the basis of which a computer programme can communicate with another programme or component, and which can also support access/data exchange internally or externally.

Automated decision-making systems

A rules-based systems that make repetitive management decisions without human intervention.

Children

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

Client

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

Consent

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

Data analytics

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

Data provenance

The origin of a piece of data and tracking of its movement across databases.

Data subject

Any individual whose personal data is used in research.

Deductive disclosure

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

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).

Non-research activity

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

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)

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

Primary data

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

Privacy

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

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

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

Profiling

The collection and processing of personal data with the intent to analyse or predict a data subject's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements in order to take direct action toward the data subject for a non-research purpose.

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

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

Researcher

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

Secondary data

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

Segmentation

An analytic technique aimed at dividing a broad target population into subsets or groups of individuals or organisations who have, or are perceived to have, common needs, interests, behaviours, and priorities, and then designing and implementing strategies to interact with them. Segmentation differs from profiling in that its focus is on well-defined groups of people with shared characteristics rather than individual data subjects.

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

Specific types of personal data that local laws require be protected at the highest possible level from unauthorized 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 or alcohol.

Vulnerable individuals

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

Web scraping (sometimes called crawling or spidering)

The use of software to extract data from websites.

4 Key Principles

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

> *1. When collecting personal data from data subjects for the purpose of research, researchers must be transparent about the information they plan to collect, the purpose for which it will be collected, with whom it might be shared, and in what form.*
>
> *2. Researchers must ensure that personal data used in research is protected from unauthorised access and/or use and not disclosed without the consent of the data subjects.*
>
> *3. Researchers must always behave ethically, comply with all applicable laws and regulations, and not do anything that might harm a data subject or damage the reputation of research.*

These principles[1] form a foundation of trust on the part of the general public, whose data we rely on, and the clients who hire us to help them make better decisions and succeed over the long-term. These principles remain as important today as at any time in our long history.

5 Research Versus Non-Research Activities

Simply put, the essential challenge researchers and those who commission research face is to ensure that data collected and processed for a research purpose is not also used for a non-research purpose without first obtaining the consent of the data subject. This distinction is more than an academic exercise. Many countries recognise the social and economic value of research and their regulatory frameworks allow for more flexibility when the purpose is research. Such as:

- *fewer restrictions on unsolicited contacts offering potential data subjects the opportunity to participate in research;*
- *extended periods of data retention (e.g. archiving);*
- *less onerous requirements when involving children and young people in research;*
- *fewer restrictions on the collection and/or use of data that may be defined as "sensitive;" and*
- *greater freedom to repurpose secondary data for research without requiring consent of the data subjects for such use, for example by defining research as a compatible purpose.*

Failure to be truthful and honest in making the distinction between research and non-research activities risks the loss of public confidence and the regulatory benefits that are essential to the long-term sustainability of research as a distinct and separate purpose.

The key distinction between research and non-research is that research limits itself to statistical/social science analysis and the delivery of insights. Its purpose is not to generate personal data or provide a basis for taking action against any specific data subject. Researchers have no interest in the identity of individual data subjects except as representatives of a larger group[2] . The identities of those whose personal data is collected and processed are not disclosed and are rigorously protected.

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

[2] *One exception is the use of personal data for quality assurance.*

Other activities may be described as research or at least seem similar to research in that people are contacted, questions asked, data recorded, and analysed. Or, existing data is enriched by harvesting data from other sources and datasets. How the data is used – the purpose for collecting it – determines whether an activity is research or something else if the purpose is to take direct action toward those individuals whose data is collected or processed, whether to change their opinions, attitudes, or behaviours or impact them in some other personalised way, then the purpose does not qualify as research.

However, this guideline recognises that there are circumstances when researchers may engage in non-research activities. When doing so they still must be transparent with data subjects about their purpose, how the data will be used, gain consent for that use, and not describe the activity as research.

6 Privacy Impact Assessments

As noted at the outset, research typically involves the collection of personal data, either directly from data subjects or indirectly through secondary data sources. In all cases, those involved have a responsibility to ensure that they do not intrude on the privacy of data subjects whose data is collected or processed. A Privacy Impact Assessment (PIA) is a useful tool for an organisation to require of its researchers when designing their research.

6.1 What is a PIA?

A PIA is a risk management tool to identify potential privacy risks to data subjects and potential legal compliance risks for the organisation. Simply stated, a PIA is a process to systematically identify and mitigate the risks to data subjects' personal data and privacy over a project's life cycle.

The design of a PIA will vary depending on the organisation's business, and its internal processes. Assessments should be conducted at the individual project level, occur in the project planning stage, and cover any planned use of personal data. A record of each assessment should be maintained, updating it as the project evolves and material changes are made to the original design.[3]

6.2 What circumstances should trigger a PIA?

Best practice would require a PIA for every project that involves the collection or use of personal data. Where that is not practical, researchers should consider particular project features that signal heightened privacy concerns and therefore require a PIA. The following list is meant only as examples and is not meant to be exhaustive:

- *any data processing on a large-scale, especially with respect to the number of data items, the number of data subjects, the planned retention period, and geographic extent;*
- *use of datasets that have been matched or combined;*
- *data collection that involves ongoing and systematic monitoring;*
- *collection or processing of sensitive data, including special categories of data, but also including financial information or data concerning criminal convictions or offences;*
- *processing that includes evaluation or scoring;*
- *processing of personal data by subcontractors;*
- *use of new technologies or methods;*
- *collection and processing of data on children or vulnerable individuals; and*
- *data transfers across borders.*

6.3 Steps in the PIA process

A PIA typically involves these four steps or stages.

[3] *For an especially useful discussion of PIAs refer to the ICO publication, Conducting Privacy Impact Assessments: Code of Practice.*

6.3.1 Chart the planned flow of information through the organisation(s)

Describe in as much detail as possible the purpose(s) for acquiring the data and how it will be collected, processed, protected, and retained. While individual organisations often have similar practices in these areas there also can be considerable variation depending on how it is structured, the operations it performs internally as opposed to working through subcontractors, the types of data being processed, and the statistical and analytic techniques used to generate the insights delivered to clients. Pay particular attention to any plans to share data with those outside the organisation (such as subcontractors or clients); uses of data in ways not reasonably anticipated by data subjects at the time of collection; and any planned processing steps that are not necessary to fulfil the purpose(s) of the research.

6.3.2 Identify potential risks, their severity and likelihood

At this stage the researcher systematically considers how the project is likely to impact data subjects' privacy. It is equally important at this stage to ensure that the project plan complies with all applicable legal requirements in those countries where data is collected or processed.

While by no means a comprehensive list, there are some obvious categories of risk that may arise from research. They include but are not limited to:

- *non-research activities that involve the use of personal data to take direct action toward an individual data subject;*
- *insufficient differentiation between research and non-research activities, thus exposing data subjects to further direct action taken towards them, including direct marketing;*
- *collection of excessive or irrelevant information (including sensitive information);*
- *overly long data retention practices;*
- *use of data for a purpose not disclosed to data subjects at the time of collection;*
- *use of data collected by subterfuge or without the knowledge of the data subject;*
- *disclosure to third parties without consent, including providing personal data back to clients;*
- *use of data subjects' comments or quotes for advertising purposes; and*
- *ineffective information security practices, such as inadequate organisational processes or those of third-party data processors, that may result in data breaches.*

Of these, the first in the list - using personal data to take direct action toward data subjects - has long been a major concern. To address it, researchers have come to rely on a rigorous consent process that, among other conditions, specifies the purpose of the collection, a description of how the data will be used, whether any of it will be shared and, if so, in what form and with whom.

6.3.3 Develop and evaluate solutions that mitigate any identified risks

This is the point at which the organisation identifies the actions it must take to address the identified privacy risks and ensure compliance with all applicable ethical and legal requirements. The ESOMAR Data Protection Checklist or national association data protection guidance are the recommended resources for solution development. It translates data privacy regulations into everyday terms to guide organisations in meeting their responsibilities within a global data protection framework. It also helps to identify gaps in the organisation's privacy protections.

While it may be fair to describe this step as a cost/benefit analysis, organisations must recognize that failing to meet its obligations to protect the privacy of data subjects can result not just in reputational damage but also in significant fines or litigation. Key to that is ensuring that all staff involved in research projects or handling of personal data regardless of source are aware of and trained in the organisation's privacy protection program.

6.3.4 Integrate risk mitigation solutions into organisational processes and plans

The final stage is the implementation of solutions into the processes to be used for the planned project as well as other similar projects.

6.4 Some specific concerns

Throughout much of its history, research has relied on primary data collection where privacy guarantees were managed via a rigorous consent process. Over about the last decade the combination of new technologies, a dramatic increase in the amount of data being collected, and increasingly innovative use of that data both for research and non-research purposes has challenged research organisations to rethink their traditional processes for protecting the rights of data subjects. Several specific concerns have emerged, and both the research sector and regulatory bodies have begun to work through solutions. The following is by no means an exhaustive list.

6.4.1 Passive data collection

Passive data collection is a widely used research approach and can include but is not limited to online audience measurement, in-store tracking, advertising testing, and attitudes and opinions about brands, products, political candidates, and so on. Common techniques used include behavioural tracking software and the use of APIs provided by a website owner.

When collecting these kinds of data, researchers must make all reasonable efforts to gain consent and limit the use of personal data to research and other legitimate research purposes. Where it is not possible to obtain consent directly from data subjects (such as when measuring traffic to a website), researchers must have legally permissible grounds to collect the data and they must remove or obscure any identifying characteristics as soon as operationally possible. In addition, prominent information about such data collection and use practices must be made available, even if indirectly, using appropriate platforms to demonstrate efforts are made to compensate for the inability to obtain consent. This could be achieved by participating in recent industry initiatives spearheaded by research industry and professional associations. These can be used to provide indirect and prominent information or opt-out mechanisms geared to data subjects.

Before web scraping is used to collect such data, researchers must consult the Terms of Use for the site as these often prohibit scraping to protect copyright or intellectual property rights.

6.4.2 Use of secondary data

Researchers and non-researchers alike increasingly look to acquire and use existing data (both public and privately held) to augment or replace primary data collection. As in the case of primary data collection, the key distinction between research and non-research is that research limits itself to statistical/social science and behavioural analysis and delivery of insights. Researchers must design their research so that further processing of the data does not risk the privacy of data subjects either directly or indirectly, for example through deductive disclosure. Organisations must put safeguards in place to mitigate the risk of such harm such as ensuring that the identity of individual data subjects is not disclosed or revealed (either directly or through combining with other data) without prior consent, using measures to reduce the granularity of the data to lower the probability of a data subject being identified, and ensuring that no non-research activity will be directed at them as a direct consequence of their data having been used for research.

6.4.3 Machine learning and other AI applications

Over about the last decade researchers have expanded their analytics techniques to include machine learning techniques to predict behavioural outcomes or build applications that automate operations such as analysis of unstructured data. Much of this work relies on large databases, often containing massive amounts of personal data. Traditional data protection principles are well-suited to protect that data, but typically do not include protections of the actual models. But these models can be reverse engineered to disclose the personal data used to train them, and even the personal data of data subjects processed when the model is in production. Techniques for defending against such intrusions are still being developed. For further discussion see the FPF report, Warning Signs: The Future of Privacy and Security in an Age of Machine Learning and the Information Commissioner’s Office (ICO) publication, Big data, artificial intelligence, machine learning and data protection. Researchers must be alert to this type of potential disclosure risk when developing their data protection infrastructures and be sure to defend against them.

6.4.4 Segmentation versus profiling

In many cases, the distinction in how personal data may be used in research versus non-research can be expressed as the difference between segmentation and profiling. Segmentation is an analytic technique that identifies a cluster of characteristics that can be used to define groups of people with common needs, interests, and priorities. Its focus is on well-defined groups of people with shared characteristics rather than individual data subjects. Most importantly, the personal data of those data subjects is not shared with clients, even when the sample used in the study may have been provided by the client. Segmentation is a legitimate research activity.

Profiling (sometimes called behavioural targeting), focuses on the collection of personal data about individual data subjects with the intent to use that data to take direct, tailored action toward them as individuals for a non-research purpose such as direct marketing. A common use is in the context of automated decision-making systems (See next section). The data may be used in research, but such research is not the primary purpose. The primary purpose is to use personal data to target individuals for a non-research purpose. Therefore, profiling is not research.

6.4.5 Automated decision-making systems

Over the last decade with the explosion of digital data of all kinds, new services have emerged that gather and analyse consumer data for a broad range of purposes, some for research, but most not. Chief among them is the development of automated decision-making systems, that is, rules-based systems that use profiles of individual data subjects to make management decisions without human intervention. Those decisions cover a wide range of activities with varying levels of impact on the privacy and well-being of individual data subjects, some of which are clearly discriminatory. They may be grouped into four broad categories:

- *Loss of opportunity (e.g., in employment, access to insurance and other benefits, housing, and education);*
- *Economic loss (e.g., granting of credit, pricing of goods and services, narrowing of choice);*
- *Social detriment (e.g., emotional duress, public embarrassment, selective advertising); and*
- *Loss of liberty (e.g. increased surveillance, incarceration).* [4]

As a result, research has been drawn into a broader discussion about the collection, use, and processing of personal data, especially when using online methods to collect behavioural data, whether by active or passive means. Some now use the term “research” to describe a data-driven industry that profiles individuals not just for marketing and sales purpose, but to automate a broad set of decisions that can affect financial well-being, health, employment opportunities, and so on. This blurring of the lines highlights the difficulty researchers face in continually demonstrating the distinction between and data analytics on the one hand, and non-research activities on the other.

Regulatory frameworks across jurisdictions may specify how this data can be used, often in terms of the severity of impacts on individual data subjects. However, organisations must not allow the personal data they collect or process to be used for any purpose that directly impacts the privacy and well-being of an individual subject.

One clear exception is the use of automated systems by researchers to promote operational efficiency and maintain data quality. These include but are not limited to sample selection, management of interviewer workload (such as call scheduling, coding of open-ended responses, data preparation, and automatic report generation). In these and similar situations the impacts on individual data subjects is not a significant concern.

6.5 Integrate risk mitigation solutions into processes and plans

The last step is to implement mitigation solutions identified by any privacy impact assessment. Each solution should be evaluated in the context of the structure of the organisation and the type of work it performs to determine whether it should be implemented for a specific project or become a standard operating procedure for all of an organisation’s research activities. As noted above, the ESOMAR Data Protection Checklist is one recommended resource. Others include DPIA guidance produced by either national associations or national data protection regulators.

[4] *For further discussion see Future of Privacy Forum (2017), “Unfairness by Algorithm: Distilling the Harms of Automated Decision-Making”.*

7 Privacy Risks Associated With Some Specific Types Of Research

Organisations must ensure that their employees are able to distinguish between valid research practices and other data collection and processing activities that have a non-research purpose, including taking direct action toward individual data subjects. This section describes a number of popular research methods, all of which are valid providing that the identities of individual data subjects are fully protected and not disclosed.

7.1 Public opinion polling

Public opinion polls are conducted to understand opinion about elections and other political topics at a given point in time. They report on a representative sample of the overall public or some particular sub-group.
However, efforts to sell products, raise funds, or promote a candidate or issue are sometimes disguised as public opinion polls or surveys. Data subjects are asked what appear to be legitimate survey questions, and they are asked to contribute money, buy a product, or add their names to a political mailing list. "Sugging" (sales under the guise of research), "frugging" (fundraising under the guise of research), and campaigning under the guise of research are not research, and researchers must not describe them as such when seeking cooperation.

7.2 Research database enrichment and data integration

Client organisations sometimes seek to enrich their customer databases with personal data gathered during a research exercise where the primary purpose is research, creating a broader basis for further research. This is legitimate research if the sole purpose is to expand the database for analytic purposes.

However, if the goal is to use the data to take direct action toward individual data subjects it is not research, and researchers must not present it as such.

7.3 Audience measurement research

Audience measurement research provides clients with aggregated statistics on the size of the audience that has been exposed to a piece of media content including advertising. This enables a media owner or advertiser to determine the value of any advertising space and is a fundamental function underpinning the provision of a wide range of services and information, particularly radio, TV and the internet.

However, if the segments reported are so detailed and granular that it is possible to target a specific data subject with content tailored to his or her individual requirements, this is profiling and therefore not research. Researchers must take the necessary care to ensure that any such data collected as part of a research project is deidentified to the maximum extent possible prior to delivery to a client.

7.4 Mystery shopping

Mystery shopping helps client organisations to determine whether the promises they make to their customers every day through advertising, branding and the launch of products and services are actually fulfilled at the point of delivery to customers. Examples of the promises may be specific prices and promotions, knowledgeable and helpful staff, clean and welcoming stores, fast telephone service and easy or intuitive online shopping. These promises are supposed to be delivered by front-line staff in physical locations, call centres and chat lines. Mystery shopping measures compliance with the promises given to customers.

Two very different types of studies may be carried out under the general heading of mystery shopping. In the first type, all personal data collected is kept confidential, not shared with the client, and used only for research purposes. In the second, personal data is not treated as confidential and is used by the client to approach data subjects individually for purposes other than scientific research (e.g. individual performance improvement or operation of a bonus system). This latter case where personal data is used for purposes other than research does not qualify as research. Researchers must take care to observe this distinction from the proposal stage through design and execution of the research.

7.5 Social media research

The largely unfiltered postings of social media users are an increasingly fruitful source of insight about a wide variety of issues of interest to companies and organisations across sectors, be they public or private. Understanding social drivers and trends at an early stage allows stakeholders to take early and timely actions.

However, much of that data is personal data in that it can be used to identify data subjects either directly or indirectly, and therefore can be used for non-research purposes. If the intent is to identify individual data subjects so that commercial messages can be targeted at them, or to quote an individual post for promotional purposes, this is not research and researchers must not describe it as such.

7.6 Online communities

Online communities are an increasingly popular method that allows brands continually to interact with groups of customers and other stakeholders across a variety of topics and thus further new product design, new services, advertising, and satisfaction over an extended period.

While many online communities are research focused, communities can also be used to purposively create brand advocates, that is, brand ambassadors who promote brands to their peers. Brand advocacy communities are normally much bigger than those for research alone and participation is intended to lead to panel members taking an action to promote the brand. Thus, advocacy panels are not research and researchers must not present it as such to community members or their clients.

7.7 Customer experience research

Customer experience research aims to collect and analyse representative sample data to understand the dynamics of satisfaction and retention for a brand/product or experience. The widespread emergence of customer experience research has resulted in new challenges in maintaining the distinction between research and non-research activities. It is increasingly common for these projects to have two purposes:

> *1. The collection and analysis of representative sample data to understand the dynamics of satisfaction and retention.*
>
> *2. Provision to the client of personal data for follow-up with service recovery, sales promotions, or product offerings.*
>
> *The first instance has a clear research purpose while the second does not. Potential exceptions include instances where the health or safety of the data subject may be at risk or other circumstances as required by law. See the following section for further discussion.*
>
> *8 Extenuating circumstances*

While they are extremely rare, there are instances in which it may be necessary and permissible to share personal data for a non-research purpose.

8 Extenuating circumstances

While they are extremely rare, there are instances in which it may be necessary and permissible to share personal data for a non-research purpose.

8.1 Protecting the health and safety of an individual data subject

On rare occasions researchers may become aware of some threat to the safety and well-being of an individual data subject where notification of a third party may seem necessary. Examples include reports of serious illness or injury, suicidal urges, malfunctioning household equipment such as a gas or electrical appliance, and so on. In such cases the researcher must first attempt to gain the consent of the data subject to involve the third party. If the data subject is unconscious or otherwise unable to reply, the researcher, after consultation with the manager overseeing the research, may notify the appropriate third party. If the data subject refuses consent, then the researcher must document the refusal and abide by the data subject's wishes.

8.2 Compelling public interest

There also may be rare occasions when sharing of personal data with government agencies without consent of data subjects may contribute to the health and safety of society as a whole. One obvious and recent example is the use of personal location data to chart the spread of the Covid-19 pandemic and monitoring of social distancing behaviours. Before complying with such requests researchers must ensure that:

- *the threat is legitimate and in the public interest;*
- *the requesting agency can provide evidence that use of the data for this purpose has been approved by the relevant data protection authorities;*
- *the requesting agency stipulates that the data will only be used for the specified purpose and not shared with other agencies or private sector organisations; and*
- *there is an agreement in place specifying the terms of sharing agreed to by both parties.*

8.3 Adverse event reporting in pharmaceutical research

Pharmaceutical research often comes with the requirement to report personal data on data subjects who, in the course of research, report adverse reactions to drugs, therapies, and other pharmaceutical products (sometimes referred to as 'adverse event reporting'). These requirements typically reflect legal requirements placed on the client organisation and tend to vary across jurisdictions. Researchers must design their research to comply with all such applicable laws and regulations. A number of research associations have developed guidelines specifying legal requirements and privacy protection guidelines, and researchers are strongly encouraged to consult them when working in this sector. They include EPHMRA, BHBIA, and Intellus Worldwide.

9 Harms Unrelated To Privacy

Finally, there are risks to the well-being of data subjects that are not privacy related, but still must be considered in the project planning stage. Organisations executing research must ensure that their employees are aware of these risks and that research is designed to guard against them.

9.1 Personal injury

Researchers must be aware of and guard against personal injury to data subjects as a result of participating in research. For example, when conducting telephone studies interviewers may contact a potential data subject who is engaged in an activity or in a setting (driving a vehicle, operating machinery, or walking in a public space) where participating might expose that individual to physical harm. A second example involves product testing where data subjects might be exposed to products that cause them physical harm, including those containing allergens, tobacco or alcohol. At the planning stage, researchers must consider these and similar risks and ensure that project personnel are given clear instructions on how to deal with such situations should they arise.

9.2 Health and well-being

Some forms of research require close personal interaction with data subjects. In such settings researchers must take all necessary precautions to guard against disease transmission in personal interview situations including inside central location settings such as focus group facilities. Potential risks run the gamut from the common cold to possibly fatal diseases, and protections should be scaled to match the severity of the disease and potential for transmission. In any situation where data subjects might be infected, researchers must take all necessary steps to prevent communication of the disease, including postponement of the interview. Interviewers and any support staff likely to come in contact with data subjects must be free of disease. Facilities must be cleaned frequently, including the use of disinfectants where appropriate. Local health authorities and industry associations are the best sources of information about the appropriate precautions in countries where research is being conducted.

9.3 Emotional distress

Researchers must exercise special care when the nature of the research is sensitive or the circumstances under which the data is collected might cause a data subject to become upset or disturbed.

9.4 Legal jeopardy

Data subjects sometimes are asked to act as data collectors by going to specific places or performing specific tasks. Examples include taking photos or making recordings in places where this may be prohibited (government buildings, banks, schools, airport security areas, private spaces or areas including shops where notices prohibiting the use of cameras are posted). Other risks include participating in or recording illegal activities, illegal drug consumption, illegally downloading website content, etc. In all such cases, researchers must ensure that data subjects are fully-informed about such risks and never given assignments that might place them in legal jeopardy.

9.5 Damage to data subjects' electronic equipment

As research increasingly relies on computers and mobile devices there is the potential to damage or impair the performance of a data subject's computer or mobile device due to software malfunction, crashing, interference with other applications, etc. Researchers must ensure that all deployed applications and systems are thoroughly tested prior to implementation, including mid-field updates, and have in place a process to respond to and address any malfunctions reported by data subjects.

9.6 Financial loss

Data subjects must not incur unreimbursed costs for participating in research. Examples include transportation costs to and from central interviewing locations or additional mobile phone charges for texting or data downloads in mobile studies.

10 References

ESOMAR Data Protection Checklist
ESOMAR/GRBN Guideline When Processing Secondary Data for Research
Future of Privacy Forum, Unfairness by Algorithm: Distilling the Harms of Automated Decision-Making
ICC/ESOMAR International Code on Market, Opinion, and Social Research and Data Analytics
ICO, Conducting Privacy Impact Assessments: Code of Practice
OECD, OECD Privacy Framework

11 Project Team

Reg Baker, North American Regional Ambassador, ESOMAR
Debrah Harding, Managing Director and Finance Director, Market Research Society
Joke Ruwen-Stuursma, Professional Standards Executive, ESOMAR

A number of individuals also provide useful comments on an earlier draft:
Pepe Aldudo, ANEIMO
Jeremy Brodsky, Gutcheck
Gerrit Burghardt, Searchlight Pharma
Jackie Lorch, Dynata
Adam Phillips, Real Research
Ashlin Quirk, Dynata
John Tabone, CRIC