



CODE OF STANDARDS AND ETHICS FOR MARKET RESEARCH AND DATA ANALYTICS

As of December, 2022

PREFACE

The Insights Association protects and creates demand for the evolving Insights and Analytics profession by promoting the indisputable role of insights in driving business impact. The Insights Association represents companies and individuals throughout the entirety of the Insights ecosystem. The Association's members may include research companies and their employees, corporate research departments and their employees, analysts, data scientists performing data analytics; organizations and individuals supporting research activities; universities, educators, and students, as well as others. Our members are the world's leading providers of intelligence, analytics, and insights into the needs, attitudes, and behaviors of populations, consumers, companies, corporate departments, and organizations. The services of our members provide decision makers with essential information with which to make intelligent decisions and deploy strategies and tactics to promote their products, services, and ideas. For purposes of this Code, the term "researcher(s)" shall refer to all of the individuals aforementioned.

The Insights Association's mission is to provide the environment and leadership that will advance the integrity, quality, and best interests of the industry and profession. The Association supports standards, guidelines, education and information resources, and self-regulation in research process, practice, and performance.

The Insights Association also works closely with other national and international associations to support and improve the integrity and quality of market research and data analytics performed for insights purposes across geographic and cultural borders.

The Insights Association Code of Standards and Ethics (the "Code") is based on the codes of founding organizations, as well as global partners and other national associations, embracing and affirming principles common to them.

PURPOSE

This Code presents the fundamental, overarching principles of ethics and professionalism for the profession and industry, establishing a platform for self-regulation that fosters confidence in the

industry and profession and ensures its continued success. Its purpose is to promote the importance and value of the work undertaken by Insights Association members and promote the interests of the industry and profession to the constituencies that they serve. A particular emphasis is placed upon the duty of care to research subjects and the protection of personal data provided by research subjects in order to comply with laws, regulations, and the ethical standards described in this code to encourage their continued contribution and cooperation. The Code is supplemented by guidelines that assist practitioners and companies with its application.

The Code covers the use of generally accepted and emerging methodologies and encourages the use of methodologies best suited to the research or business problem at hand.

The Code recognizes the global nature of the industry and profession and the requirement to comply with all applicable state, national, and international laws and regulations.

This Code will be reviewed regularly by the Insights Association Standards Committee.

INTERPRETATION

This Code sets the standards of professional and ethical conduct for all Insights Association members and the research and data analytics industry and profession.

In the event of a conflict between this Code and applicable law, the more restrictive standard governs. This Code is to be interpreted in conjunction with other relevant guidelines and principles. These and other supplemental documents are referenced at the end of this document.

The Code has been organized into sections describing the responsibilities of members. The Code is not intended to be, nor is it, an immutable document. Circumstances may arise that are not covered or that may call for modification. The Code, therefore, seeks to be responsive to the changes in market research and data analytics without favoring any approach, with broad recognition that innovation will continue to drive the evolution of insights sourcing. The Standards Committee and Board of Directors of the Insights Association will evaluate these changes and, if appropriate, revise the Code.

Adherence to the Code is required by all members of the Insights Association. The Insights Association requires its members to review and attest to this Code as part of their membership application and annual membership renewal. In so doing, members grant the Insights Association the authority to enforce the Code and will cooperate with the Association's enforcement efforts. Information regarding enforcement may be found in the Enforcement section at the end of this document. The Association's Standards Committee is available to address any complaints and alleged breaches of the Code.

Throughout this document, the word "must" is used to identify principles and practices that researchers are obliged to follow. The word "should" indicates recommended practices.

DEFINITIONS (Glossary)

For the purposes of the Code, the following terms have these specific meanings:

Child – Individual for whom informed consent to participate in research must be obtained from a parent or legal guardian. Definitions of the age of a child vary substantially and are set by national laws and self-regulatory codes.

Client – Any individual, organization, department or division, internal or external, that requests, commissions or subscribes to all or any part of a research project.

Consent – Voluntary, informed agreement by a person (research subject or legal guardian) for participation in research and/or the collection and processing of their personal data. This consent is based upon the person having been provided with clear information about the nature and purpose of the data being collected or used, with whom it will be shared and how it will be used. Depending on applicable law and regulation, particularly with consent for children or other vulnerable individuals, such consent may need to be verifiable.

Data analytics – The process of examining data sets to uncover hidden patterns, unknown correlations, trends, preferences and other useful information that can be used to describe, understand, influence and predict behaviors. Data analytics also includes data integration, which is the process of integrating data from different sources.

Data Science – A field of activity or discipline that employs mathematics, statistics, and computer science, incorporating techniques like machine learning, cluster analysis, data mining, predictive analytics, and visualization.

Harm – Tangible and material injury (such as physical injury or financial loss), intangible or moral damage (such as damage to reputation or goodwill), unsolicited personally-targeted marketing messages, or excessive intrusion into personal life.

Non-research activity – Taking direct action toward an individual whose data was collected or analyzed with the intent to change or persuade the attitudes, opinions, or actions of that individual. Non-research activities include but are not limited to advertising, direct marketing, and automated decision-making.

Passive data collection – The permission-based or ethical collection of data by researchers observing, measuring, recording, or appending a research subject's actions or behavior for the purpose of research and without direct interaction with the research subject.

Personal data (which may also be referred to as Personally identifiable information or PII) – Information that can be used to distinguish or trace the identity of an individual, either alone or when combined with other identifying information, either directly or indirectly. Personal data can include information such as name, social security number, date and place of birth, mother's maiden name, biometric records, photographs, sound or video recording, geolocation data, and other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Privacy policy (sometimes referred to as privacy notice) – A published summary of an organization's privacy practices describing the ways an organization gathers, uses, discloses, and manages research subjects' personal data.

Primary data – Data directly collected from or about a research subject for the purpose of research.

Research – All forms of market, opinion, and social research and data analytics used in the systematic gathering and interpretation of information about individuals and organizations. It uses the statistical and analytical methods and techniques of the applied social, behavioral, and data sciences to generate insights and support decision making by providers of products, services, and ideas, which also includes governments, non-profit organizations, and the general public.

Research subject – Anyone from whom data are collected or used for research purposes.

Researcher – Any individual or organization carrying out or acting as a consultant on research, including those working in client or corporate research departments, as well as subcontractors.

Secondary data – Data collected by another party, whether for a research or non-research purpose, and data that have already been collected and are available from another source.

Sensitive data – Specific types of personal data that local laws require be protected from unauthorized access to safeguard the privacy or security of an individual or organization to the highest possible standards. The definitions of sensitive data vary by jurisdiction. In the U.S., sensitive data includes health and financial data. In other jurisdictions, like the EU, sensitive data includes racial or ethnic origin, health records, sexual orientation or sexual habits, criminal records, political opinions, trade association membership, religious or philosophical beliefs, location, financial information, and illegal behaviors such as the improper use of regulated drugs or alcohol.

Subcontractor – A service provider executing any element of a research or data analytics project on behalf of another entity. Individual contractors are considered subcontractors. Subcontractors engaged in research and/or analytics are considered researchers.

Vulnerable individual (may also be referred to as vulnerable people or populations) – Person who is permanently or temporarily unable to represent their own interests through a mental, emotional, societal or physical cause that may limit their capacity to make voluntary and informed decisions or are in a role or position where they may be pressured to participate or answer in a specific way.

FUNDAMENTAL PRINCIPLES OF THE CODE

The Code is based on the following principles:

1. Respect research subjects and their rights as specified by law and/or by this Code.
2. Be transparent about the collection of personal data; only collect personal data with consent and ensure the confidentiality and security of such data.
3. Act with high standards of integrity, professionalism, and transparency in all relationships and practices.
4. Comply with all applicable laws and regulations, as well as applicable privacy policies and terms and conditions, that cover the use of research subjects' data.

Section 1: Duty of Care

Researchers must:

1. Balance the interests of research subjects, research integrity, and business objectives with research subjects' privacy and welfare being paramount.
2. Be honest, transparent, fair, and straightforward in all interactions.
3. Respect the rights and well-being of research subjects and make all reasonable efforts to ensure that research subjects are not harmed, disadvantaged, or harassed as a result of their participation in research.
4. Always distinguish between research and non-research activities so as to maintain public confidence in the integrity of research.
5. When engaging in non-research activities, do not permit any direct action toward an individual based on their participation in research without their consent. Such consent can enable non-research activities to utilize research techniques for certain types of customer satisfaction, user, employee, and other experience activities.
6. Ensure that data obtained for purposes of research are not used to reveal the identity of the research subject without their consent.

Section 2: Primary Data Collection

Transparency, Notice and Choice

Researchers must:

1. Promptly identify themselves so that research subjects can easily verify researcher identity and credentials.
2. Respect the right of research subjects contacted for research as part of a customer list to know the sponsoring company (company that provided their personal data to the research company) at the end of the research or at the beginning (understanding that disclosure may preclude the research subject from participating in the research).
3. Clearly state the general purpose of the research as soon as methodologically possible.
4. Ensure that participation is voluntary and based on accurate information about the general purpose and nature of the research.
5. Respect the right of research subjects to refuse requests to participate in research.
6. Respect the right of those already engaged in research to terminate their participation or refuse requests for additional or other forms of research participation.
7. Upon request, permit research subjects to access, correct, or update any personal data being retained about them.
8. Limit the use of incentives only as a means to encourage participation in research.
9. Work with research subjects and all stakeholders to resolve any issues or concerns that may arise as a result of participating in research.

Consent

Researchers must:

1. Obtain the research subject's consent for research participation and the collection of personal data or ensure that consent was properly obtained by the owner of the data or sample source.
2. If known at the time of data collection, inform research subjects of any activities that will involve re-contact. In such situations, the researcher must obtain the research subject's consent to share personal information for re-contacting purposes. Re-contacting research subjects for quality control purposes does not require prior notification.
3. Allow research subjects to withdraw their consent at any time.
4. Obtain consent from the research subject prior to using his/her data in a manner that is materially different from what the research subject has agreed.

Section 3: Passive Data Collection

Researchers must obtain consent when collecting and/or using passive data whenever possible, regardless of method employed. In such situations, researchers also must provide clear and simple methods for research subjects to grant and retract their consent. If a device is shared by multiple individuals, every effort should be made to delete data that is not sourced from the individual that gave consent. Where it is not possible or practical to obtain consent, researchers must have legally permissible grounds to collect the data and must remove or obscure any identifying characteristics as soon as operationally possible.

Section 4: Use of Secondary Data

When using secondary data as defined in the glossary that includes personal data, researchers must:

1. Ensure that the data was not collected in violation of restrictions imposed by laws or regulations, or in ways that were not apparent to or reasonably understood or anticipated by the research subject.
2. Ensure that the use is not incompatible with the purpose for which the data was originally collected.
3. Ensure that use of the data will not result in any harm to research subjects and there are measures in place to guard against such harm.

Section 5: Data Protection and Privacy

Researchers must:

1. Have a privacy policy that is easily accessible and publicly available (if appropriate), is easily understood and clearly states their data protection and privacy practices.
2. Only share a research subject's personal data with a third party under the following conditions:
 - a. with the research subject's consent; or
 - b. in limited situations as permitted by applicable data protection law and regulation
3. Only use or share personal data for the purpose(s) for which it was collected.
4. Ensure that data collected as part of the research process is not used to identify a research subject without their consent, or as required to comply with applicable law and regulation.
5. Ensure that all personal data collected, received, or processed by the researcher, subcontractor or other service provider is secured and protected against loss, unauthorized access, use,

modification, destruction, or disclosure by the implementation of appropriate information security measures.

6. Limit data collected to what is necessary for the specific research and analytical requirements.
7. Ensure that personal data is retained only for the duration required for the intended purpose and in compliance with applicable contracts, policies, laws, and regulations.
8. Inform research subjects of any non-research use prior to data collection and obtain their consent.

Section 6: Children and Vulnerable Individuals

Researchers must take special care when conducting research with children and other vulnerable individuals. When conducting a research project with such individuals, researchers must:

1. Follow the laws and regulations governing consent for children or vulnerable individuals, both as it pertains to age and the type of research being conducted.
2. Take special care when considering whether to involve children and young people (minors) in research. The questions asked must take into account their age and level of maturity.
3. Obtain verifiable informed consent from a parent or legal guardian for children or other vulnerable individuals when required.
4. Ensure that vulnerable individuals are not unduly pressured to cooperate in research and can provide independent responses with no harm due to their vulnerability.
5. Consider the topic of the research and the vulnerable person's ability to give consent, and their capacity to participate truthfully and openly without the possibility of harm.

RESPONSIBILITIES TO CLIENTS

Section 7: Honesty and Transparency

Researchers must:

1. Be honest and transparent in all interactions.
2. Accurately represent their qualifications, skills, experience, and resources.
3. Identify subcontractors upon request, where possible without creating a competitive disadvantage or conflict of interest. Ensure that subcontractor practices and associated contracts comply with this code.
4. Inform all clients when a project is conducted on behalf of more than one client.
5. Not use any data collected solely for a specific client for any other purpose without permission from that client, except as it pertains to internal quality and operational processes.
6. Maintain data and research materials in compliance with applicable laws and regulations, industry quality standards, company processes, or as requested by a specific client.
7. Make a full citation of any secondary data to properly credit the source of the information used.
8. Work in good faith to resolve all disputes with clients, subcontractors, and research subjects.
9. Be transparent about non-research activities in which a sample or panel may participate.

Section 8: Research Quality

Researchers must:

1. Design or assist clients in designing effective research and clearly communicate any issues or limitations that may be associated with a chosen research design.
2. Perform all work in accordance with the specifications detailed in the research proposal or statement of work.
3. Perform all work in accordance with generally accepted research practices and principles. When using new and emerging research practices, researchers must ensure that the underlying principles are methodologically sound.
4. Ensure that findings and interpretation are adequately supported by data and provide such supporting data to the client upon request.
5. Provide the technical information required to permit the client to verify that work meets contract specifications, while protecting personal information (refer to Section 2: Primary Data Collection, Consent, #2 for more information).
6. Provide sufficient information to permit independent assessment of the quality of data presented and the validity of conclusions drawn.
7. Not misrepresent the scope of their expertise, training, and experience.
8. Be transparent when discussing any known or suspected substantive biases in the research.

RESPONSIBILITIES TO THE PUBLIC

Section 9: Research for Public Release

Researchers must:

1. Always obtain clear approval from clients to release findings publicly.
2. Ensure that the findings released are an accurate portrayal of the research data, and that careful checks are performed on the accuracy of all data presented.
3. Provide the basic information, including technical details, to permit independent assessment of the quality and validity of the data presented and the conclusions drawn, unless prohibited by legitimate proprietary or contractual restrictions.
4. Make best efforts to ensure that they are consulted as to the form and content of publication when the client plans to publish the findings of a research project. Both the client and the researcher have a responsibility to ensure that published results are not misleading.
5. Not permit their name or that of their organization to be associated with the publishing of conclusions from a research project unless those conclusions are adequately supported by the data.
6. Promptly take appropriate actions to correct information if any public release is found to be incorrect.

RESPONSIBILITIES TO THE PROFESSION

Section 10: Professional Responsibilities

Researchers must:

1. Comply with this Code and research industry codes of conduct in countries where the research is conducted.
2. Comply with all applicable international, national, state, and local laws and regulations.
3. Act with high standards of integrity, professionalism, and transparency in all relationships and practices.
4. Behave ethically and do nothing that might damage the reputation of research or lead to a loss of public confidence in it.
5. Communicate with respect and civil discourse in all interactions.

ENFORCEMENT

Enforcement of the Code is the responsibility of the Insights Association Standards Committee (the “Committee”). Investigations into a Code violation may come as a result of a complaint that is filed or for any other reason deemed appropriate by the Insights Association. Investigations will include direct contact with the member involved in a Code violation complaint.

Investigations that find a failure to abide by this Code may result in sanctions ranging from the issuance of a private written warning to public expulsion from the Insights Association.

Compliance and enforcement deliberations are confidential and will not be disclosed to anyone other than those needing access to the information to enable them to formulate expert opinions.

Filing a Complaint

Any person, company, or organization affected by an alleged violation of the Code may file a complaint. Should the Committee be aware of circumstances where the risk of reputational damage to the profession warrants, the Committee may initiate its own investigation. The identity of anyone filing a complaint will be kept anonymous throughout the enforcement process.

Complaints against a member may also be filed by contacting the Insights Association at enforcement@insightsassociation.org or (202) 800-2545.

Complaints must include the following information:

- Statement of the case
- The Code section(s) allegedly violated
- Supporting documents and other evidence
- Name and contact information of the complainant
- Name and contact information of alleged violator(s)

Enforcement Process

On receipt of a complaint, the Insights Association CEO or designee, after consultation with the Committee chair, will examine possible Code violations to establish or confirm the facts and circumstances of the complaint, including involving the alleged violator(s). If the CEO determines there is merit to the complaint, it will be assigned to the Standards Committee for further review. If the Committee determines that a breach may have occurred, the alleged violator is provided with a written description of the complaint including supporting documentation, naming the Code provisions allegedly violated, and the name of the complainant.

The Committee may notify company employers of any allegations regarding Code violations by employees. The employer may participate in the enforcement process and designate a contact with the knowledge and authority to represent the employer.

A complete complaint will be adjudicated, resulting in outcomes ranging from dismissal to sanction to request for remedial action to prevent recurrence. The Committee will allow the violator to respond, to which the Committee will reply. The Committee's decision may be appealed to the Insights Association Board of Directors. Costs incurred in defense of an alleged violation will not be reimbursed.

Upon review of a complaint, the Committee will recommend one of the following outcomes:

- Take no action: there is either insufficient evidence or no breach of Code
- Impose one or more sanctions based on the seriousness of the breach

Sanctions

The Committee may impose the following types of sanctions:

- **Warning** – An unpublished notification of concern or breach.
- **Reprimand** – A published censure, to include a letter detailing the violation(s) of the Code and the consequences to be expected if the violation(s) are repeated.
- **Suspension** – Suspension of membership in the Insights Association for a minimum of one year. At the end of the suspension, the member may be reinstated by the Committee if remedial action has been taken and documented to ensure that the violation(s) named in the complaint will not be repeated. If remedial action is not taken or is considered insufficient, the Committee may consider expulsion.
- **Expulsion** – Expulsion of membership for a minimum of two years. After that period, they can apply for reinstatement and must provide written assurance that remedial action has been taken to ensure that the violation(s) named in the complaint will not be repeated.

Public Disclosure

The cause, circumstances, and sanctions imposed by the Committee may be published by the association and noticed to peer associations or other bodies:

- Publication may include a summary of the decision, the name of the violator, and the sanction.
- The complainant's name will not be included in the publication of a sanction unless specifically requested by the complainant.

Notification to Authorities

Suspected violations of law may be brought to the attention of relevant public authorities and/or enforcement bodies.

Further Measures Authorized by the IA Board of Directors

In exceptional circumstances, the Committee may request the Board of Directors to authorize further measures it deems necessary.

SUPPLEMENTAL GUIDELINES

Joint guidelines published by ESOMAR and GRBN*:

- The ESOMAR/GRBN [Online Research Guideline](#)
- The ESOMAR/GRBN [Guideline on Online Sample Quality](#)
- The ESOMAR/GRBN [Guideline on Duty of Care](#)
- The ESOMAR/GRBN [Mobile Research Guideline](#)
- The ESOMAR/GRBN [Guideline on Children, Young People, and Vulnerable Individuals](#)

[AAPOR Code of Professional Ethics and Practice](#)

[EphMRA Code and Guidelines](#)

[Intellus Worldwide Standards and Guidelines](#)

[ISO 20252, Market, opinion and social research, including insights and data analytics – Vocabulary and service requirements](#)

[ISO 27001, Information technology – Security techniques – Information security management systems – Requirements](#)

[16 CFR Part 312 - Children’s Online Privacy Protection Rule \(COPPA\) \(FTC\)](#)

[45 CFR Part 46 - Protection of Human Subjects \(Common Rule\) \(HHS\)](#)

[20 CFR Part 50 - Protection of Human Subjects \(FDA\)](#)

*The Insights Association is a founding member of GRBN (Global Research Business Network).