CODE OF STANDARDS AND ETHICS FOR MARKET RESEARCH AND DATA ANALYTICS

September 2025

PREFACE

The Insights Association advances and protects the Insights and Analytics profession by championing the critical role of insights in driving business success. Representing the full breadth of the ecosystem—research firms and corporate teams, analysts, data scientists, educators, students, and supporting organizations—our members are global leaders in understanding people, markets, and organizations.

Our mission is to uphold the integrity, quality, and impact of the profession. We provide standards, guidelines, education, and self-regulation to support best practices, while protecting both practitioners and the research participants who make insights possible.

The Association also collaborates with national and international partners to strengthen the quality and integrity of research and analytics worldwide.

The Insights Association Code of Standards and Ethics ("the Code") builds on the principles of our founding organizations and global partners, affirming our shared commitment to ethical and responsible practice

PURPOSE

This Code represents the fundamental, overarching principles of ethics and professionalism for the industry, establishing a platform for self-regulation and ensuring confidence in the way research data is collected and conclusions drawn. 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 research participants and clients they serve. Particular emphasis is placed upon our duty of care to research participants and the protection of their data, ensuring their continued trust in and cooperation with our profession described in this Code.

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.

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 annually 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. Enforcement information 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 researchers are obliged to follow. The word "should" indicates recommended practices.

DEFINITIONS (Glossary)

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

Artificial Intelligence – a set of technologies designed to simulate and predict human intelligence and problem-solving capabilities.

Child – an 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 state and national laws and self-regulatory codes.

Client – an 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 creating, combining, and interrogating data sets to uncover patterns, correlations, trends, preferences and other useful information that can be used to describe, understand, influence and predict attitudes and behaviors.

Generative AI – refers to artificial intelligence models that can create *new* content or data based on patterns learned from existing datasets.

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 including but not limited to advertising and direct marketing.

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 research and without direct interaction with the research subject.

Personal Data – information that can be used to distinguish or identify an individual, either alone or when combined with other information, either directly or indirectly. Generally, aggregate, deidentified, pseudonymized, and anonymized data are not considered personal data.

Privacy Policy (or Privacy Notice) – a published summary of an organization's privacy practices describing the ways an organization gathers, uses, discloses, and manages research participants' personal data.

Primary Data – data collected to address the specific business information needs of a single organization.

Research – includes all forms of market, opinion, and social research, including data analytics applied for research purposes, is the systematic gathering, analysis, and interpretation of information about individuals and organizations. It uses the statistical and/or analytical methods and techniques of the applied social, behavioral, data, and other sciences to generate insights and support decision-making by providers of goods and services, governments, non-profit organizations and the general public.

Research Subject – a human from whom data are collected or used for research purposes, either through active participation or passive observation.

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 – collected for one or more purposes with potential applicability to future business information and decisions support situations.

Sensitive Data – types of personal data that local laws require to 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.

Subcontractor – a service provider executing any element of a research or data analytics project on behalf of another entity. Individual contractors are considered subcontractors.

Synthetic Data – artificially generated data that mimics real-world datasets.

Vulnerable Individual (also referred to as vulnerable people or populations) – a person who is permanently or temporarily unable to represent their 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 feel 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, regulation, 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 in transit and at rest.
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 in all business practices.

Section 1: Duty of Care

Researchers must:

1. Balance the interests of research subjects, research integrity, and business objectives.
2. Respect the wishes and rights of research subjects and make reasonable efforts to ensure that research subjects are not harmed, disadvantaged, or harassed as a result of their participation in research.
3. Be honest, transparent, fair, and straightforward in all interactions.
4. Always distinguish between research and non-research activities to maintain legislative and 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.
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 business credentials.
2. Respect the right of research subjects contacted for research as part of a customer list to know the sponsoring company (the company that provided their personal data to the research company) either at the beginning or end of the research (with the understanding that disclosure may preclude participation).
3. Be fully transparent with research participants regarding relevant parameters and requirements of a research project.
4. The researcher must notify the data subject at the beginning of the research when there is use of an AI-based avatar or chatbot for data collection which could be perceived to be a human.
5. Ensure participation is voluntary and based on accurate information, stated as soon as

methodologically possible, about the general purpose and nature of the research.

6. Respect the right of research subjects to refuse requests to participate in research.
7. Respect the right of those already engaged in research to terminate their participation or refuse requests for additional or other forms of research participation.
8. Upon request, permit research subjects to access, correct, or update any personal data being retained about them.
9. Limit the use of incentives only as a means to encourage participation in research.
10. 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 confirm 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. Obtain consent from the research subject before 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 informed consent before collecting or using passive data whenever feasible, regardless of the collection method. Participants must have clear, accessible options to grant and withdraw consent at any time. If a device is shared among multiple users, researchers must take all reasonable steps to delete data not linked to the consenting individual. In cases where obtaining consent is impractical, data collection must be legally justified, and personally identifiable information must be removed, pseudonymized, or anonymized as soon as operationally possible. Researchers must implement safeguards to mitigate the risk of unintended data capture and ensure compliance with applicable privacy laws and ethical standards.

Special considerations must be given to the collection of sensitive data, ensuring stricter security, limited retention, and explicit participant awareness. Data accuracy must be validated to account for device limitations, software conflicts, and other factors that may impact reliability.

Section 4: Artificial Intelligence

Artificial Intelligence (AI) research tools present incremental and evolving considerations that impact respondent privacy, transparency, data integrity, and potential for bias.

1. Respondent anonymity is essential across the data lifecycle. Personal data should not be used in AI training data sets without informed consent, and researchers must ensure personally identifiable information cannot be reverse-engineered by AI inference.
2. If AI tools are selected then their use, purpose, technique (e.g., predictive, generative), model-type (open-source or proprietary), model-accuracy, and data source (primary, secondary, synthetic) must be disclosed. AI-generated data, either predictive or generative, must be clearly distinguished from data directly derived from human research participants.
3. No AI system used in research should operate exclusively without human judgment embedded in its lifecycle — from design and implementation to validation and application. AI models must be evaluated regularly to consider intentional and unintentional biases in data and design. Researchers should evaluate if the model reflects its intended purpose and consider bias resulting from demographic or cultural variables.

Section 5: Use and Integration of Data

When using second- and third-party data, researchers must:

1. Take reasonable steps to confirm the data was not collected in violation of laws or regulations, or in ways that were not apparent to or reasonably understood or anticipated by the research subject.
2. Ensure the use is not incompatible with the purpose for which the data was originally collected and to which research subjects consented.
3. Ensure use of the data will not result in any harm to research subjects and there are measures in place to guard against any such harms.
4. Be transparent about any underlying data set, including its origins, use rights, custodianship, structure, populations represented, recency, and intellectual property ownership considerations.

Section 6: Data Protection and Privacy

Researchers must:

Have a privacy policy that is readily accessible, easily understood, and clearly states both the Researchers' privacy practices and the Research subject's privacy rights.

1. Before transferring personal data to a client, subcontractor, or other third-party must:
    a. Obtain the research subjects' consent (unless an applicable law or regulation allows or requires otherwise)
    b. Ensure such recipients maintain at least equivalent security measures, and have committed to comply with applicable data protection and data breach laws;
    c. Take particular care to ensure that the data protection rights of data subjects whose

personal data is transferred from one jurisdiction to another are maintained;
   d. Transfer only the minimum amount of personal data necessary for such recipients to perform the agreed services.

2. Only use or share personal data for the purpose(s) for which it was collected.
3. Ensure that data collected as part of the research process is not used to identify a research subject without their consent, unless required to comply with applicable law and regulation.
4. 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 organizational and technological controls.
5. Limit data collected to what is necessary for or reasonably likely to benefit the specific research and analytical requirements and objectives.
6. 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.
7. In the event of a data breach involving personal data, data subjects, along with any relevant authorities, must be informed of the breach as required by applicable laws and contracts.

Section 7: Children and Vulnerable Individuals

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

1. Follow the laws and regulations governing consent for children or vulnerable individuals, as it pertains to age, the type of vulnerability, and the research being conducted.
2. Take special care when considering whether to involve children or vulnerable people in research. The questions asked must take into account their age and level of comprehension.
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 or misled to cooperate in research.
5. Consider the topic of the research and the vulnerable person's ability to give consent, and then only move ahead if the participant has the capacity to participate truthfully and openly without the possibility of harm.

RESPONSIBILITIES TO CLIENTS

Section 8: Honesty and Transparency

Researchers must:

1. Be honest and transparent in all interactions.
2. Accurately represent their qualifications, skills, experience, and resources.
3. Be transparent about the origins of the data being used and any use of AI that may represent a risk to research quality or accuracy.
4. Ensure the full disclosure of any personal, financial, or organizational conflicts of interest that might influence the research.

5. Identify subcontractors upon request, when possible without creating a competitive disadvantage or conflict of interest, or when required by contract. Ensure that subcontractor practices and associated contracts comply with this code.
6. Inform all clients when a project is conducted on behalf of more than one client.
7. Use data collected solely for a specific client only for its intended purpose and for that client except as it pertains to internal quality and operational processes.
8. Appropriately cite any secondary data to properly credit the source of the information used.
9. Work in good faith to resolve all disputes with clients, subcontractors, and research subjects.
10. Be transparent about non-research activities in which a sample or panel may participate.

Section 9: Research Quality

Researchers must:

1. Design or assist clients in designing effective research that is fit for purpose and communicate any issues or limitations that may be associated with a chosen research design.
2. Perform all work under the specifications detailed in the research proposal, statement of work, and any documented, post-proposal amendments to the research design.
3. Perform all work under 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. Be transparent when discussing any known or suspected substantive biases in the research.

RESPONSIBILITIES TO THE PUBLIC

Section 10: Research for Public Release

Researchers must:

1. Obtain explicit approval from clients before releasing findings publicly.
2. Ensure the findings released are an accurate portrayal of the research data, are not presented in a way that is likely to mislead, 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. Promptly take appropriate actions to correct information if any public release is found to be incorrect.

RESPONSIBILITIES TO THE PROFESSION

Section 11: Professional Responsibilities

Researchers must:

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

ENFORCEMENT

Enforcement of the Code is the responsibility of the Insights Association Standards 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 company or individual 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 the parties involved and those needing access to the information 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 investigation. The identity of anyone filing a complaint may be kept anonymous if needed to protect the complainant.

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 will examine possible Code violations to establish or confirm the facts and circumstances of the complaint, including consultation

with the alleged violator(s). If this examination determines that 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 (unless anonymity is needed to protect the complainant).

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

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, after which the decision is final with no further recourse. Costs incurred in defense of an alleged violation or as the result of sanctions 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 notified 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.