

CODE OF STANDARDS AND ETHICS FOR
MARKETING RESEARCH AND DATA ANALYTICS

APRIL 2019



PREFACE

The Insights Association represents companies and corporate research, insights and data analytics departments, and individuals working in the marketing, opinion and social research and data analytics industry and profession. Our members are the world's leading providers of intelligence, analytics and insights into the needs, attitudes and behaviors of consumers, companies 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.

The Insights Association was founded in 2017 with the merger of CASRO, a trade association formed in 1975, and MRA, a professional society founded in 1957. The Insights Association, established to foster and promote the interests of the industry and profession, serves organizations and their research-related employees including researchers, analysts and data scientists, as well as individual research professionals not affiliated with member organizations. The Association's members may include research companies and their employees, corporate research departments and their employees, analysts, data scientists generating data analytics, organizations and individuals supporting research activities, universities, educators and students, as well as others. 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 marketing 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 both CASRO and MRA. The Code also draws on the ICC/ESOMAR Code and the codes of other national research associations, embracing and affirming principles common to them.

PURPOSE

This Code presents the fundamental, overarching principles of ethics and professionalism for the industry. 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, with a particular emphasis on the protection of personally identifiable information provided by data subjects to comply with laws and regulations and encourage their continued contribution and cooperation. Further, the Code seeks to establish a platform for self-regulation, building on the successful efforts of CASRO and MRA, to foster confidence in the industry and profession and ensure its continued success.

The Code is supplemented by guidelines that assist practitioners and companies with its application.

The inclusion of data analytics in the Code recognizes changes in the industry and profession and the proliferation of data that has resulted in a changing role for members and the services they

provide. 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 annually by the Insights Association Standards Committee.

INTERPRETATION

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

In the event of a conflict between this Code and applicable law, applicable law shall govern. 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 marketing 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 mandatory requirements, a principle or practice that researchers are obliged to follow. The word "should" indicates a recommended practice.

DEFINITIONS

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

Children – Individuals for whom 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. In the U.S., a child is defined as being age 12 and under. In the EU, a child is defined as being age 16 and under with derogations permitted for member states to set different age definitions. In the absence of a definition in a country, a child is defined as being age 12 and under where consent by a parent or legal guardian required and a "young person" as age 13 to 17.

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 for participation in research and/or the collection and processing of their personally identifiable information (PII). This consent is based upon the data subject 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.

Corporate researcher – An individual or department in a company or organization that commissions or carries out research or acts as a consultant on research that is for internal use by that company or organization.

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, artificial intelligence, cluster analysis, data mining, predictive analytics and visualization.

Data subject – Anyone from whom data, which may include PII, are collected or used for research purposes. In cases where the data subject actively engages in research, a data subject may also be referred to as a research participant.

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

Non-research activity – Taking direct action toward an individual whose data, which may include PII, was collected or analyzed with the intent to change 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 – The collection of personal data by observing, measuring or recording an individual's actions or behavior. Passive data may contain PII.

Passive data collection – The collection of data by observing, measuring, or recording a data subject's actions or behavior without direct interaction with the data subject.

Personally identifiable information or PII (referred to as personal data in the EU and other jurisdictions) – Information that can be used to distinguish or trace the identity of an individual, either alone or when combined with other personal or identifying information. PII 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 data subject's PII.

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

Research – All forms of marketing, 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, also including governments, non-profit organizations and the general public.

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 any subcontractors used.

Secondary data – Data collected by another party, whether for a research or non-research purpose, and subsequently used in research. Secondary data may contain PII.

Sensitive data – Specific types of PII 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 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 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.

Vulnerable individuals (may also be referred to as vulnerable people or populations) – Individuals who may have limited capacity to make voluntary and informed decisions.

FUNDAMENTAL PRINCIPLES OF THE CODE

The Code is based on the following principles:

1. Respect the data subjects and their rights as specified by law and/or by this Code.
2. Be transparent about the collection of PII; only collect PII with consent and ensure the confidentiality and security of PII.
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 data subjects' data.

Section 1: Duty of Care

Researchers must:

1. Prioritize data subject privacy above business objectives.
2. Be honest, transparent, and straightforward in all interactions.
3. Respect the rights and well-being of data subjects and make all reasonable efforts to ensure that data 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 (for example, promotional or commercial activities directed at data subjects, including but not limited to advertising and direct marketing), do not permit any direct action toward an individual based on his or her 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.

Section 2: Primary Data Collection

Transparency, Notice and Choice

Researchers must:

1. Promptly identify themselves to data subjects so that the participants can easily verify researcher identity and credentials.
2. Clearly state the general purpose of the research as soon as methodically possible.
3. Ensure that participation is voluntary and based on accurate information about the general purpose and nature of the research.
4. Respect the right of data subjects to refuse requests to participate in research.
5. Respect the right of those already engaged in research to terminate their participation or refuse requests for additional or other forms of research participation.
6. Upon request, permit data subjects to access, correct or update any PII held about them.
7. Limit the use of incentives only as a means to encourage participation in research.

Consent

Researchers must:

1. Obtain the data subject's consent for research participation and the collection of PII 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 data subjects if there are any activities that will involve re-contact. In such situations, the researcher must obtain the data subject's consent to share PII for re-contacting purposes. Re-contacting data subjects for quality control purposes does not require prior notification.
3. Allow data subjects to withdraw their consent at any time.
4. Obtain consent from the data subject prior to using his/her data in a manner that is materially different from what data subject has agreed.

Section 3: Passive Data Collection

The collection of data by observing, measuring, or recording a data subject's actions or behavior] must whenever possible be based on the consent of the data subject. In such situations, researchers must provide clear and simple methods for data subjects to grant and retract their 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, researchers must:

1. Ensure that the use is not incompatible with the purpose for which the data was originally collected.
2. 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 data subject.
3. Ensure that the use is compatible with the consent obtained when the data was collected.
4. Honor all data subject requests that their data not be used.
5. Ensure that use of the data will not result in any harm to data subjects.

Section 5: Data Protection and Privacy

Researchers must:

1. Have a privacy policy that is easily available (including being publicly available if appropriate) and clearly states their data protection and privacy obligations and practices.
2. Only share a data subject's PII with any third-party¹:

¹ Note: A subcontractor is a third-party.

- a. With that data subject's consent; or
 - b. In limited situations that are in the interest of the data subject or the public. Such limited situations include, but are not limited to: adverse event reporting, health and safety, and situations pursuant to required legal process.
3. Ensure that all PII collected, received or processed by the researcher or any subcontractor or other service provider is secured and protected against loss, unauthorized access, use, modification, destruction or disclosure by the implementation of information security measures required by applicable laws and regulations.
 4. Limit data collection to what is necessary for the specific research and analytics purposes.
 5. When collecting PII for research that may also be used for non-research activities, inform data subjects of any non-research use prior to data collection and obtain their consent for any non-research activity.
 6. Comply with all applicable international, national, state and local laws and regulations, and local codes of conduct with respect to PII and the local variations in the definition and requirements for sensitive data.

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. Obtain verifiable consent from a parent or legal guardian for children or other vulnerable individuals when required.
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. When working with other vulnerable individuals, researchers must follow all applicable laws and regulations and ensure that such individuals are capable of making informed decisions and are not unduly pressured to cooperate in research.

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. Upon request, inform the client if any part of the work is subcontracted.
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.

6. Retain all data and research materials in compliance with applicable laws and regulations, industry quality standards, company processes or as requested by a specific client.
7. Work in good faith to resolve all disputes with clients, subcontractors and data subjects.

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 accepted research practices and principles. When new and emerging research practices are used, 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 PII (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.

Note: Subcontractors engaged in research or analytics activities are considered researchers.

RESPONSIBILITIES TO AND OF CORPORATE RESEARCHERS

Section 9: Corporate Researchers

Corporate researchers play multiple roles in the industry and profession; they may be clients, researchers, or both. Corporate researchers must always comply with all applicable requirements of this Code.

RESPONSIBILITIES WITH RESPECT TO SUBCONTRACTING

Section 10: Subcontracting

Researchers and subcontractors must:

1. Ensure that subcontractors are provided the appropriate level of information so that the researcher and the subcontractor can make an informed decision as to the subcontractor's suitability for participation.

2. Ensure that any potential conflicts are disclosed and resolved before any research engagement.
3. Ensure that the parties maintain the confidentiality and security of confidential and proprietary information, including PII, which was provided by either party.
4. Not use the confidential and proprietary information of either party, including PII, illegally or contrary to the agreement under which confidential or proprietary information was obtained.
5. Document all work and confidentiality requirements with written agreements that protect the interests of clients, researchers and subcontractors.

RESPONSIBILITIES TO THE PUBLIC

Section 11: Research for Public Release

Researchers must:

1. Always obtain clear approval from clients to release findings publicly.
2. Ensure that the findings they release are an accurate portrayal of the research data, and that careful checks on the accuracy of all data presented are performed.
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.

LEGAL REQUIREMENTS

Section 12: Legal Requirements

Members must:

1. Comply with all applicable international, national, state and local laws and regulations, and research industry codes of conduct in countries where the research is conducted.
2. Not engage in any acts of bribery or induce any party to engage in illegal behavior.

RESPONSIBILITIES TO THE RESEARCH PROFESSION

Section 13: Professional Responsibility

Members must:

1. Comply with this Code.
2. Act with high standards of integrity, professionalism and transparency in all relationships and practices.
3. Engage in competitive practices that are reasonable in view of the interests of those competing and the public and do not include practices condemned by law as hostile to the public interest.

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.

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 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 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 within 20 business days, resulting in dismissal to sanction to request for remedial action to prevent recurrence. The Committee will allow the violator 20 business days to respond, to which the Committee will reply within 20 business days. This schedule may be suspended until the resolution of an external legal case related to the complaint. 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.

Sanctions

The Committee may impose the following types of sanctions:

- **Warning** – An informal notification of condemnation.
- **Reprimand** – A formal censure.
- **Suspension** – Suspension of membership in the Insights Association. At the end of the suspension, the member may be reinstated by the Committee if remedial action has been taken 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** – If a member is expelled, they can apply for reinstatement no less than one year after expulsion and must provide a 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.

SUPPLEMENTAL GUIDELINES

The following provide supplemental guidance for specific research applications:

- Joint guidelines published by ESOMAR and GRBN²:
 - The ESOMAR/GRBN Online Research Guideline
 - The ESOMAR/GRBN Guideline on Online Sample Quality
 - The ESOMAR/GRBN Guideline on Duty of Care (In development)
 - The ESOMAR/GRBN Mobile Research Guideline (To be released shortly)
 - The ESOMAR/GRBN Social Media Research Guideline (In development)
 - The ESOMAR/GRBN Guideline on Children, Young People, and Vulnerable Individuals
- AAPOR Code of Professional Ethics and Practice
- EphMRA Code and Guidelines
- Intellus Worldwide Code 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

² The Insights Association is a founding member of the Global Business Research Network (GRBN).