Infinite Insight Data Privacy Statement

Introduction:

As a market research and opinion polling agency, the privacy of our respondents is a prime concern. Members of the public will only voice their opinions if they can be certain that no breach of confidentiality will occur.

From its inception in 2010, Infinite Insight has firmly committed to complying with the ICC/ESOMAR Code of Practice and the Market & Social Research Association's (MSRA) Code of Ethics. Since it came into effect in 2018, Infinite Insight has voluntarily complied with the General Data Protection Regulation (GDPR) by the European Union in those African countries, which have not yet formulated their own country-specific guidelines.

Since the Data Protection Act of 2019 has come into effect in Kenya, Infinite Insight is complying with the regulations laid out therein.

Definitions:

1. Infinite Insight Ltd. (also "We", the "Company") is registered in Kenya as a research agency; we engage in market, social, and public opinion research. We operate on the basis of a research permit, issued annually by NACOSTI. The Company is not involved in e-commerce or any type of marketing activity which involves the sale of personal details to third parties.
2. "Respondents" are defined as members of the public, who have given their consent to participating in a research project.
3. "Staff" of Infinite Insight includes directors, permanent employees, and temporary contract staff, including field interviewers, moderators, and external consultants.
4. "Clients" are defined as local and international companies, research agencies, or academic institutions, who commission us to provide research services in Kenya. Such research services include consumer research, public opinion polls, and social research.

Section I: Research Activities

Data Collection:

Infinite Insight collects data in three major ways:

1. Personal Interviews (F2F: face-to-face): respondents are randomly selected, following probability sampling techniques. Interviews occur at private homes or respondents' place of work. Remote interviewing via Zoom, Teams, Skype, WhatsApp, etc. is an extension of personal interviewing.
2. Telephonic Interviews (CATI): respondents' phone numbers are randomly generated (i.e. random digit dialing), at times supplemented with geographically targeted calling among respondents, who had given prior Informed Consent to be contacted for telephonic interviews.
3. Online Interviewing (CAWI): Links to the survey are sent to randomly generated phone numbers, or emailed to respondents, who had given their Informed Consent to being contacted; in addition, links may be posted on social media.

Participation in all research projects is voluntary. Respondents must give prior Informed Consent to participation; in telephonic surveys, Informed Consent can be given verbally, once the Informed Consent statement has been read out aloud and the respondent has understood its content.

Data Collection among Minors:

In the case of minors (respondents below the age of 18), parents or legal guardians are required to have given their consent to their wards' participation.

Contact details (personal identifiers) of minors will only be retained for verification and quality control purposes; once this has been completed, they will be deleted.

Should we, at any time, learn that a minor has been interviewed without parental consent, all data (identifiers, classification data, and survey responses), will be deleted.

Parental consent is a necessary condition, but not a sufficient one; i.e. underage respondents retain their right to refuse answering all or part of the questionnaire.

Types of Data Collected:

There are three categories that are collected in a research project:

1. Personal Information (Identifiers):

Identifiers include respondents' names, addresses, phone numbers, and email addresses. These data are collected only for Quality Control purposes. All personal identifiers are kept separated from the bulk of the survey data and can only be linked via serial numbers. Should verification reveal that data were collected erroneously, fraudulently, or without Informed Consent (or if Consent is revoked at this stage), both survey responses and contact information will be deleted with immediate effect.

Once the veracity of an interview has been established, the Data Processing Manager will permanently delete these identifying data. Thereafter, survey data cannot be traced back to any individual respondent. Nobody, including Infinite Insight Staff, will be able to ascertain who gave what answers.

Respondents' identifiable information may only be shared and/ or retained, if:

- The Respondent has expressly consented to sharing with a third party or retaining identifying information for a specified purpose and for a specified period of time.
- If Follow-up surveys are part of the project design, this will be clearly explained; the Informed Consent Form will explicitly request permission to re-contact respondents for a follow-up survey.
- If respondents also choose to sign up for future projects and have their contact details entered in a general respondent database (e.g. panel), a second Informed Consent Form will be required. Respondents may revoke consent at any time; their contact details will be deleted from the project-specific and general databases.

2. Classification Data (Demographics):

Classification data include sex, age (or age band), marital status, ethnicity, religious affiliation, socio-economic status, occupation, affiliation to a political party, or product category usage; these will be used to analyse demographic sub-groups within aggregated data sets. Respondents are free to refuse to respond to any given question. Demographic data cannot be traced back to any individual, as respondents are distinguished only by serial number, not personal identifiers.

3. Survey Responses:

Survey Responses comprise all opinions or behaviours volunteered by the respondent during an interview. These data are of interest only in aggregated form. Various statistical operations can be performed to establish group behaviour or preferences; thus, while collective tendencies can be established, no prediction on the behaviour or opinions of any given respondent can be made.

Data Retention Schedule:

Type of Data:	Retention Period:	Comments:
Identifiers (Contact Details)	2 weeks Alternatively, if Informed Consent has been given, for the duration of the project.	Identifiers will be deleted as soon as the commissioning client has accepted the data and all queries on data collection have been resolved; this typically occurs within two weeks following completion of fieldwork. If Informed Consent has been given to retain contact information to allow follow-up surveys, identifiers will be stored for the duration of the project.
Classification Data & Survey Responses	Minimum of 1 Year	Aggregated anonymised data is retained for two purposes: (1) To assist clients with data analysis, when in need of information on local context. (2) To facilitate longitudinal studies (tracking of consumer habits or public opinion)
Reports & Presentations	Indefinite	Analytical reports and graphic presentations are based on aggregated data; they never contain identifiers. These reports and presentations are archived permanently (see section on Data Security).

Purpose of Data Collection:

Data collected during fieldwork is analysed to provide insights on trends among Kenyan consumers and Kenyan general public. These include the establishment of category usage or brand shares; media usage; opinions on national or international issues.

Data collected in Kenya is processed in Kenya; commissioning clients only receive the analytical reports and aggregated anonymised data in electronic format. Data are transferred using secure transfer protocols (e.g. DropBox).

Data Processing & Data Security:

In field, irrespective of data collection mode, data collection platforms (e.g. Dooblo Survey to Go) are used. Interviewers log in with their ID and password; then interviews are uploaded onto a cloud server upon completion; all information on the interview is automatically deleted from the device at that moment.

Only the Data Processing Manager has access to the cloud server. At the end of each day, the data is downloaded to his system; in the process, all data will be removed from the cloud server.

The DP system is password-protected; data is stored on an external device (and therefore, inaccessible to online incursions). The DP manager will assign contact details to Field for quality control. The cases for verification consist only of contact details and do not contain respondents' confidential answers to the questionnaire. Upon verification, contact details will be permanently deleted.

The survey data (excluding identifiers) are stored on an offline external device in the office of the Managing Director.

Infinite Insight adopted a home-office policy at the start of the pandemic. This policy was made permanent in 2021. Hence, all systems are decentralized; hence, risk of intrusion by unauthorized outsiders is minimised. Individual systems are protected by Windows/Apple firewalls as well as anti-

virus and anti-malware software (MalwareBytes or equivalent). All security packages are kept up-to-date at all times.

Data back-ups are done using external devices that are offline, once the back-up has been concluded. Infinite Insight uses no cloud storage. Cloud services are used for secure data transfers to commissioning clients (DropBox). Data files are always compressed (WinZip) and are locked with strong passwords prior to transfer, following guidelines on password strength provided by our IT Consultant (combination of capital and miniscule letters, special characters, and numbers).

Since 2014, Infinite Insight has adopted data collection on mobile devices. Paper documents, such as lists or questionnaires, do not accrue to the same extent as in the past. Paper documents, such as Informed Consent Forms, corporate records, tax records) are stored in strongboxes in a secured storage room at the house of the Managing Director.

Cookie Policy:

On our home page (www.infiniteinsight.net), no cookies are used; we do not track page traffic or conduct page analytics.

In online surveys, cookies will be deployed by our cloud service provider only to prevent multiple entries.

Summary of Respondents' Rights:

1. Participation in surveys and polls is always voluntary.
2. Respondents will always be informed about the purpose of the survey and on how the data will be processed; i.e. in anonymised aggregated form.
3. Respondents will be informed about why we collect some identifying data (name and contact information); these will be used for quality control purposes and will be deleted from the data once interviews have been verified as legitimate.
4. If a respondent withholds Informed Consent, no interview will be conducted.
5. Respondents may revoke Informed Consent at any time during the interview; respondents may also refuse to respond to any question they object to.
6. If a respondent has voluntarily signed up for follow-up projects or future surveys, he/she may withdraw that consent at any time; contact and classification data will be removed from the data file.

Section II: Employees' Data Privacy

In compliance with the Data Protection Act, and The Employment Act (Amendment) Act of 2022, Infinite Insight maintains all personal data of its employees within individual **Employee Personnel Files** which are securely stored with access to only authorized personnel within the Company. All collection and processing of information and data contained within the Employee Personnel File is in accordance with the employees' right to privacy.

All data and information is lawfully and legitimately collected and not used for purposes other than as outlined within this Policy document.

The Employees' Personal data consensually collected from the employee and stored in individual employee personnel files include:

- Physical address and location of place of residence
- Bank account details
- Personal Identity Number (PIN)
- Identification Document (ID)
- Next of Kin contact (Name, Telephone, mobile and address)
- Curriculum vitae and education certificates
- Your Photo, Picture, Image

New Employees are requested to provide personal information prior to the confirmation of employment. Employees are further requested to periodically verify and update their personal data to ensure its accuracy and that any inaccurate personal data is promptly deleted or rectified.

Additional information contained within Personnel Files include:

- Employment Contract & terms of employment (Job description)
- References
- Award and Disciplinary records
- Leave applications
- Performance reviews
- Promotion and Salary adjustments
- Health history and records consensually and voluntarily by the employee or from a third party such as a medical service provider

An employee is provided with a copy, or original of all documents generated by the Company and held within an employee's file. The information contained within the employee's personnel file is limited to its relevance and necessity for the purpose of which it may be required or processed.

Data and information contained within Employee Personnel files are a documented written history of the employment and are maintained for the employees' Employment Lifecycle and duration of employment.

Personal Data Access

- Personnel files are accessed and used by the Accounts and Administration Department for HR and Payroll purposes. The Finance/ General Manager has sole custody of all personnel files.

- No employee personal information is shared or accessed by third parties without express consent of the employee, or where the company may be legally required to provide personal employee information.
- Infinite Insight has no **third party** arrangements where employee personal information is shared within or outside of Kenya.
- In the event that any such personal employee information is required to be transferred to a third party within or outside of Kenya, full informed consent from the employee must be obtained.
- Proof of adequate data protection and safeguards for the transport of any such data will be made available to the employee.

Personal Data Storage and Safety

- Security measures are put in place to ensure the physical or electronic employee personal information is securely stored within the company's physical or digital secure storage space.
- Infinite Insight Limited acknowledges the right of the employee to exercise their rights in relation to the personal data collected and the duties of Infinite Insight as the employer in relation to the use of the employee's personal data and actions to be taken in the event of a personal data breach.
- The employees' Personnel file is kept and maintained for the duration of employment. Where an employee ceases to be an employee of Infinite Insight Limited and all contractual obligations cease, the employee's personnel file is retained for a further period of 36 months.

Transparency and Employee Awareness

- In addition to the Company's Data Protection and Privacy Policy and The Kenya Data Protection Act, the Employee is expressly informed and made aware of the Company's Privacy Policy through:
    - The employee's Letter of Employment,
    - Employment Induction
    - The Company's HR Manual
- All documents express and outline the employees' requirements of full compliance to the Privacy Policy.
- Staff Training sessions are held regularly:
    - Annual MSRA Ethics Training for all staff; this includes data privacy regulations that must be adhered to.
    - Project briefings and training sessions always contain the MSRA Ethics Training, including the sensitization to data privacy regulations.

Employees Obligations to Infinite Insight' Clients

- It is expressly outlined, the employees contractual and legal obligations to the privacy and security of personal data of the **company's customers / respondents**, obtained through the performance of the employee's contractual duties.
- Any personal data of the company's customers/ respondents, otherwise or fraudulently obtained by the employee and used or shared contravening or breaching the Company's Data Privacy Policy, or the Data Protection Act, may face prosecution for data protection breaches.
- It is thus expressly outlined that an employee can face prosecution for data protection breaches whether they be in the conduct of employment or due to fraudulent activities.

Section III: Data Privacy Officer & Handling of Complaints

The Role of the Data Protection Officer

- Infinite Insight has appointed a **Data Protection Officer**.
- The officer monitors Company compliance with the regulations of the Data Protection Act internally.
- The officer serves as a liaison between the company and members of the public; i.e. would be tasked with addressing possible privacy concerns directed at the company.

Dispute Resolution:

The Data Protection Officer serves as liaison between the public and the company. And if privacy concerns arise, it will be the Data Protection Officer's task to see that a revocation of Informed Consent will be acted upon without delay. If a respondent had previously agreed to participate in future research projects, but has changed his/her mind, the Data Protection Officer will assure that Name, Phone Number, Address, and Email Address are deleted from the database with immediate effect.

Contact Us:

For any questions regarding our data privacy policies, contact us on dpo@infiniteinsight.net

Or contact us by mail or phone:

Data Protection Officer
Infinite Insight Limited
Mirage Tower 2, Pent Floor, Room 32
Chiromo Road

P.O. Box 1324, 00606 Nairobi
Tel: +254 774157784