



DATA PROTECTION POLICY

Last Updated: 01 January 2021

Objective: Establish a consistent Data Protection Policy (“Policy”) to be administered by Mobile Accord, Inc. (T/A GeoPoll)

Scope: This Policy applies to all departments and all persons working for GeoPoll.

Authority: The Chief Executive Officer, the General Counsel, and/or their nominee are responsible for the development, administration, and evolution of this Policy (“Authority”). Each person / department at GeoPoll is responsible for compliance.

Statement and Objective of this Policy: GeoPoll is a global research organization that conducts market research studies through several channels including voice call interviews, in-person interviews, 2-way SMS messages, web links, and mobile applications. GeoPoll maintains certain policies to guide its employees with respect to legal and regulatory requirements and standards of conduct required in areas where improper activities could jeopardize our stakeholders, including but not limited to the respondents GeoPoll engages with, as well as GeoPoll. GeoPoll recognizes the risk involved to participants of our research services (respondents). The purpose of this Policy is to affirm the required standards and establish the required practices by which GeoPoll adheres to and upholds the same. This Policy and the rules it outlines are intended to protect the data of respondents through transparent and informed consent policies, the secure storage and transmission of data, and the safeguarding principles for children and the other respondent populations that may or may not otherwise participate in GeoPoll exercises.

Purpose of data collection: The research studies GeoPoll facilitates cover a range of topics based on the needs of our clients. GeoPoll works closely with all clients on questionnaire development and study implementation and will not administer studies which could cause harm to the respondent. Furthermore, in studies conducted using traditional telecommunications network modes (SMS), GeoPoll also works closely with our Mobile Network Operator (MNO) partners to ensure compliance with local regulations and content norms.

Transparent and Informed Consent: The transparent and informed consent of all respondents who choose to participate or not to participate in GeoPoll data collection exercises is the foundation and bulwark upon which GeoPoll operations and is in line with industry-best standards, and applicable laws and regulations that exist today.

Procedures for Obtaining Consent: All GeoPoll research studies include a fully transparent informed consent (i.e. opt-in / opt-out) process. The specific process varies on the channel through which research is conducted and all surveys begin with an opt-in. During the opt-in process, the respondent is provided information about GeoPoll’s intent to survey them anonymously and confidentially and asked to consent to participate. This process is free to the respondents, robust, compliant with IRB human subject research standards, and further customizable based on client wishes.

SMS and link-based surveys include an opt-in message which a respondent must respond to in order to proceed with a survey. Voice call and in-person interviews also include a consent statement which respondents must agree to before proceeding. Interviewers for voice call and/or in-person studies go through a robust training procedure to ensure they understand the importance of obtaining consent and applicable human subject research standards before proceeding with an interview.



Procedures for withdrawing consent: Respondents can opt-out from any study and are also given instructions on how to blacklist themselves from future studies if they do not wish to be contacted. In addition, respondents may request that their Personal Identifiable Information (“PII”) and any related data are deleted / expunged from GeoPoll’s database.

Due to the multiple channels through which GeoPoll conducts research studies, the process through which respondents can remove consent vary based on the research methodology:

SMS and Web Links: Respondents who respond “HELP” via SMS are provided with a mechanism to blacklist themselves directly via SMS and are also provided a link to GeoPoll’s privacy policy which includes additional information on how their data is used and how to request data be removed. Web link surveys include a link to GeoPoll’s website and privacy policy.

Voice Call Interviews: Following a voice call survey, all respondents who participated in the survey are sent a SMS message which has information on GeoPoll and a link to GeoPoll’s privacy policy for more information. In the event that clients request a voice call line be set up for inquires for a specific project, GeoPoll can facilitate that request and provide that phone number in an SMS message or to respondents during the initial survey. Costs for establishing such a voice call line are typically borne by the client and call cost borne by the respondent. Furthermore timelines for establishing the same vary from market-to-market.

In Person Interviews: When interviews are conducted in person, GeoPoll interviewers will share information on how to contact GeoPoll in the form of a physical copy of the GeoPoll Privacy Policy and/or information on how to access the Privacy Policy.

Obtaining Consent from Children or At-Risk Adults Unable to Provide Consent: In the case that GeoPoll cannot obtain informed consent, GeoPoll will obtain consent from a parent or guardian where appropriate. For additional information see the safeguarding section below.

Types of information we collect and store:

Personal Identifiable Information (PII):

Personal Identifiable Information includes any information about a respondent that could be used, either individually or in combination, to identify an individual. It may be directly identifiable information such as name or address, and indirectly identifiable information such as gender, age, and location. Examples of PII that GeoPoll may collect include:

- Mobile phone number
- Gender
- Age or date of birth
- Sub-national location
- Household size

Sensitive Personal Data (SPD) (e.g. religion, sexual orientation, etc.):

For certain studies GeoPoll may collect sensitive personal data that warrants even stricter security and confidentiality procedures. This data may include:



Racial or ethnic origin

- Physical or mental health information
- Sexual orientation
- Political affiliation
- Religious or philosophical beliefs
- Refugee displacement status

Storage and Usage of PII and SPD:

The above data types are stored securely according to the procedures outlined in the data storage section below. GeoPoll employees are granted access to individual study data on an as-needed basis.

Retention of Information and Data Ownership:

As policy GeoPoll securely stored client data and respondent PII and/or SPD for 3-10 years. For the avoidance of doubt, and in accordance with industry best standards, GeoPoll treats respondent PII and/or SPD as belonging to the respondent. Client data and respondent PII and SDP can be expunged and/or destroyed at any time upon request by the relevant party. Such requests from clients can be addressed to the Client Services team. For respondents wishing for their PII and/or SPD to be expunged and/or destroyed, an email can be sent to legal@mobileaccord.com requesting the same.

Usage of information for future studies:

Standard demographic information such as gender, age, and location information collected in one survey or interview may be used to contact respondents for future studies they may be eligible for, provided they have not opted-out of future studies.

Anonymizing of records:

GeoPoll's system assigns all respondents a unique identifier and does not share mobile phone numbers with clients or third parties.

Safeguarding for Children and At-Risk Populations

GeoPoll does not engage in survey research with children under the age of 15. For respondents between 15-18 years and adults at risk and/or otherwise lacking capacity, GeoPoll will exercise the following safeguarding principles:

- GeoPoll does not act in any way that take responsibility or decision making away from the research subjects.
- Any activity that involves adults at risk or children will have a risk assessment exercise carried out in anticipation to determine compliance with legal norms.
- If any information collected that shows a child or adult at risk is in an unsafe situation, GeoPoll will work with the client or organization supporting the activity to take action and reduce the risk. Since GeoPoll does not have a physical presence in many countries, we will rely on our partners to support such activities and take appropriate action.

Data Storage and Access:



- **Physical Security**
 - All systems and servers are securely backed up on a nightly basis to encrypted off-site storage with an RPO of 24 hours, and servers and employee laptops use hard drive encryption and run antivirus / anti-malware software regularly per industry standards.
- **Technological Security**
 - Data is protected including utilizing encrypted, high-availability servers stored within a secure datacenter.
 - Encryption of the personal information while in transit through the https protocol.
 - Encryption of the personal information while at rest.
 - Encryption of the backups including personal information.
 - Personal information stored on secured servers and infrastructures.
 - All systems and services undergo penetration tests on a quarterly basis.
- **Organizational Security**
 - Confidentiality clauses in all of our employment and service agreements with natural or legal persons having access to personal information.
 - Computers and eGeoPoll accounts of all of our employees being password protected.
 - Access to GeoPoll accounts being protected by unique login details and passwords that are required to be changed regularly.
 - All employees and contractors undergo background checks prior to employment.
- **Third-Party Policies, Data Sharing, and Data Processing**
 - Adherence with third-party data protection and privacy policies that are required by law in any and all applicable jurisdictions.
 - Obliging third-party partners and vendors to adhere to, comply with, and sign on to all GeoPoll data protection and privacy policies.
 - GeoPoll requires any third-party partner and/or vendor to sign legal documents (i.e. Vendor Services Agreements, Data Process Agreements, and the like) which oblige them to adhere to GeoPoll data protection and privacy policies.

Data Sharing and Data Processing:

Disclosure: All apparent breaches of this Policy and/or noncompliant acts must be disclosed to the Chief Executive Officer, the General Counsel, and/or their nominee for review and determination of whether a violation of this Policy exists.

Complaints or Inquiries: All complaints or inquiries concerning possible violations of this Policy should immediately be reported to the Chief Executive Officer, the General Counsel, and/or their nominee for review and a determination as to whether a violation of this Policy exists.

Violations: In addition to any compensatory and/or punitive damages contained in any provision of law that may be relevant to this Policy, any determination by the Authority that a breach or a noncompliant act has occurred or may occur may result in immediate termination of an employee's employment with GeoPoll, an order that the employee remove himself/herself from the activity causing the violation, and provide GeoPoll with evidence of such removal, or an order that the employee ceases and desists from engaging in the noncompliant act and evidence of the same. In the event of termination for violation of any provision of this Policy, the employee shall expressly acknowledge that he/she shall not be liable to receive from GeoPoll any form of severance or termination payment. Furthermore, GeoPoll reserves the



right to take recourse to its legal rights under any applicable law and/or regulation to the fullest extent of the law.

Integration: The terms contained in this Policy is indoctrinated into GeoPoll policy and shall be integrated into all employees' terms of employment which govern the arrangement between GeoPoll and the employees.

Understanding: Each employee shall read through this Policy and confirm his/her understanding and acceptance of the same, as well as the principles, terms and conditions contained within this Policy. All employees are charged with having read and understood this Policy

This Policy is officially accepted and implemented by GeoPoll.

Nicholas Becker – CEO
Mobile Accord, Inc. (T/A GeoPoll)

RELATED POLICIES & PROCEDURES (all policies are reviewed every two (2) years):

- Data Classification & Protection Policy
- GeoPoll Privacy Policy