KANTAR GLOBAL SURVEYS

PRIVACY NOTICE FOR KANTAR SOUTH AFRICA

Last updated: Oct 2026

Introduction

This Privacy Notice sets out the commitment of Kantar, and all its affiliate Kantar Group companies (altogether, “Kantar”, “we”, “our” or “us”), to the participants of our research surveys (“respondent”, “respondents” or “you”), and governs respondents’ rights regarding privacy and data protection. A full list of relevant Kantar Group companies can be found at www.Kantar.com/Surveys-data-controllers.

This privacy policy is applicable to online survey research, telephone survey research, postal, face to face interviews and other market research methodologies conducted by Kantar. Learn more about Kantar at www.Kantar.com. This Privacy Notice explains how we collect, store and use the personal data you provide when taking part in our research surveys.

The latest version of this Privacy Notice is publicly available on the Kantar South Africa website at https://www.kantar.com/privacy-south-africa.

For individuals located in South Africa, Kantar South Africa (Pty) Ltd processes personal information in accordance with the Protection of Personal Information Act, 4 of 2013 ("POPIA"). This Privacy Notice is intended to provide the information required under POPIA and to explain how we collect, use, disclose, retain and protect personal information in connection with our market research and related activities.

We often conduct market research for our own purposes, in which case Kantar is the “data controller and responsible business (or similar term) for the purposes of applicable data protection law. When we conduct market research for our clients, Kantar and its clients may both be the data controller (or similar term) for your personal data. However, sometimes we conduct market research on behalf of our clients who have provided us with your contact details (for example, you are a customer or employee of our client), in which case the sole data controller (or similar term) party is our client and Kantar is acting as a “data processor” and service provider, on behalf of its client. Our client may also have provided you with their own privacy notice or related information about the processing of your personal data on their behalf. Where our client is a data controller and responsible party for your personal data, their identity may be revealed to you at the end of the survey to protect against bias for the purposes of accurate market research.

For the purposes of this Privacy Notice, “personal data” means any data or information that relates to an identified or identifiable living individual (or the equivalent applicable term in your jurisdiction).

Taking part in our research activities is entirely voluntary; you may decline to answer any questions and you can withdraw from surveys at any time. If you choose not to provide certain personal information, withdraw your consent (where consent is relied upon), or discontinue participation, you may be unable to take part in the relevant research study, receive any associated incentive or reward, participate in follow-up research activities, or receive services that depend on the provision of such information.

By participating, you confirm that you have read and understood the terms of this Privacy Notice.
We ask you to read this Privacy Notice carefully.

Lawful Collection and Use of Data

We have contacted you to take part in a survey by telephone, post, face to face or online by:

- Receiving your contact details from the client we are conducting the survey for, with whom you may either be registered, employed, received products or services from or generally dealt with
- Receiving your contact information from a Kantar panel or a third party, such as a research panel or sample provider that you have registered with or been in contact with. In most cases for online surveys, we do not receive your contact information and the panel or third party simply invites you to join our survey
- Sourcing your information from publicly available resources or randomly generated telephone numbers, where we have a genuine market research purpose for contacting you
- Receiving your contact details from a previous survey, where you have agreed to be re-contacted by us to possibly participate in further surveys

We collect your personal data in several ways such as through our website(s) (for example a survey portal), our mobile applications and other activities such as social media, apps and online, face to face or telephone studies or other research activities. We may add other ways and activities moving forward but we will always operate in compliance with this Privacy Notice.

We have set out below, more detailed information about how we use your personal data. Some data protection laws require that we have a "lawful basis" for our processing, which is a legal justification that has been pre-defined by the relevant law for collecting, storing and using personal data. For your information where that requirement exists, we have set out below the relevant lawful basis alongside the applicable purpose. The legal bases we commonly use are listed below and could be different for each use case:

- we have your consent for the use of your personal data;
- we need to use your personal data in order to perform a contract with you; or
- we need to process your data to comply with a legal obligation;
- the use of your personal data is necessary for our (or our clients') legitimate interests (in which case we will explain what those interests are).

If you receive an email that concerns you, purporting to be from us, please let us know as shown below in the *"How to Contact Us"* section of this Privacy Notice.

Case	Purpose	Personal data	Source	Legal basis
Providing you with information	Provide you with information regarding surveys, panel arrangements, incentive schemes, products or services that you request from us, or that we have determined may be of interest to you.	Name, email address, IP address, phone number, postal address, job title	We obtain this data from you directly, for example when you download reports or other content from our website, or when you make an enquiry with us.	We will seek your consent or we have determined that we have a legitimate interest in using your details to provide you with relevant information. You can withdraw your consent or opt out of communications from Kantar at any time.
Recruiting you for market	To contact you and invite you to participate in market research surveys (as described below).	Name, email address, phone number, postal address, other	We obtain this information directly from you, our client(s) or from	We rely on your consent which has been collected by us, by our client(s)

research surveys		demographic information relevant to a survey (i.e., age, job title, etc.)	third party recruitment organisations such as research panels or sample providers for which you have opted-in or registered. In limited circumstances, we obtain this information from publicly available sources.	or by third parties for this purpose. In limited circumstances, we rely on our and/or our clients' legitimate interest to recruit survey participants.
Market research surveys	To understand your views about certain products and services or to understand your behaviour in different situations. To validate answers you gave in a recent survey we conducted. To administer participation e.g. prize draws, incentives, pre-tasks etc. To re-contact you e.g. for ongoing and follow-up surveys. In certain cases, we will use artificial intelligence (AI) tools or chatbots to interact with you and/or process your personal data for the market research. Where relevant, we will take appropriate measures to ensure that you know that you are interacting with a smart tool or chatbot.	Identifier, name, email address, voice, image, gender, date of birth, nationality, opinion and general survey responses, and where permitted, personal data that is protected by applicable law, including information concerning your race or ethnicity, religious or philosophical beliefs, sex life or sexual orientation, health or social background	We obtain this data from you directly	Voluntary participation in survey whereby we ask for your consent to collect and use your personal data
Fraud Protection	Protection of our business interests against fraudulent behaviour	IP address, browser specifications, device specifications, postal addresses, email addresses, official identification number	We obtain this data from you directly	Legitimate interest – we and/or our clients have a legitimate interest in protecting our business against fraud or other prohibited behaviour
Survey Participation Uniqueness	Prevention of multiple entries in surveys by the same individuals	IP address, browser specifications, device specifications	We obtain this data from you directly	Legitimate interest – we and/or our client(s) have a legitimate interest in preventing multiple entries by the same individual

Data Matching and Enrichment	We enrich the data we hold about you by matching your personal data with data obtained from third parties. This will help us to improve your profile and ensure that we select relevant surveys for you. We utilize matching services (i.e. third parties who are specialized in data management) to acquire additional information about you from public and private data sources (such as social networks, retailers and content subscription services with whom you have an account) or to use your personal data as an aid to develop additional or new types of anonymous data sets (i.e. we compile your aggregate data with data from other consumers to create a new lifestyle segment). The matching service (our data partner) holds the personal data we share for a short time, uses it to assemble the additional information, and then returns the combined information to us. Data partners are contractually bound to delete the data we share with them and/or are not authorised to use it in any way other than for this specific purpose.	Persistent unique identifier, contact details, email address, social login, cookie, mobile device ID, official identification number	We obtain this data from you directly or combined with other secondary databases	Consent if applicable to the research objectives in a survey you participate in, we will only perform data matching techniques using 3rd parties with your consent
Managing online or telephone survey opt-outs	When an individual has requested not to be contacted again, we hold their details to enable this	Contact details, name, e-mail address, telephone number	We obtain this data from you directly	Compliance with a legal obligation to honour your right not to be contacted
Facial Expression	To understand your reaction and views about certain products and services or to understand your behaviour in different situations. Facial expression data may be collected in some surveys. We will always	Facial expression	We obtain this data from you directly	Consent if applicable to the research objectives in a survey you participate in, we will only collect facial coding data with your consent

	ask your permission to record this data.			
Eye Tracking	To understand your visual attention while shown a marketing campaign. Eye tracking data may be collected in some surveys. We will always ask your permission to record this data.	Eye movement	We obtain this data from you directly	Consent if applicable to the research objectives in a survey you participate in, we will only collect eye tracking data with your consent
Disclosure to Authorities	To share or disclose pursuant to judicial or other government subpoenas, warrants, orders or pursuant to similar and other legal or regulatory requirements, we will provide such information to the appropriate authorities	Identifier, name, contact details, email address, incentive received	We obtain this data from you directly, or combined with other secondary databases	Legal obligation
Business Transactions	We may need to transfer our data to other organisations to manage a business transition or financial transaction, such as a merger, acquisition, divestiture, restructuring, reorganisation, dissolution or sale of all or some of our assets	Name, email address, postal address, mobile device ID, demographics, any detail you share with us about yourself and your household, and all person data we hold for you as described above	We obtain this data from you directly or from the sources described above	Where necessary to comply with a legal obligation, or legitimate interest – we have a legitimate interest to conduct and manage Kantar business transactions.

For South African data subjects, Kantar processes personal information in accordance with the lawful justification grounds recognised under POPIA, including:

- the consent of the data subject;
- the conclusion or performance of a contract;
- compliance with a legal obligation;
- the protection of a legitimate interest of the data subject;
- the pursuit of Kantar's legitimate interests; and
- any other lawful justification recognised under POPIA.

Incentives and Rewards

To incentivise you to participate in the market research surveys, (where you are a panel member) the panel of which you are a member, or our clients, may reward you with prize draws, vouchers and other incentives. Any incentive program is subject to their applicable terms and conditions of the relevant survey. In such cases, we will inform those third parties of your completion of a particular survey to manage the incentive process. Your incentive may be subject to particular terms and conditions, such as those from any panel you are a member of.

Third Parties (Clients and Suppliers)

We may share your personal data (including your sensitive personal data) with companies in the Kantar Group and our third-party vendors and processors for survey-related purposes, such as data processing, and fulfilment of prize draws or other incentives. This could also include vendors managing or assisting us in managing our survey platforms and databases, marketing automation and CRM, quality checks and fraud prevention, and customer care. Some vendors will specifically work with us on enriching your survey responses, allowing us to select you for surveys, such as vendors specialized in, but not limited to, data matching, online ad effectiveness measurement, and social media data interactions. Categories of personal data shared with these vendors would typically be, but may not be limited to, your name, email address, postal address, phone number, cookie ID, panellist ID (where applicable), IP address and the information you submit in our market research surveys.

Kantar Group companies and our third-party data partners, platforms and websites are all contractually bound to keep any information they collect and disclose to us, or that we collect and disclose to them, confidential and must protect it with security standards and practices that are equivalent to our own.

We do not sell your personal data (including your sensitive personal data) and have not done so in the last 12 months. Kantar may collect your personal data in collaboration with its client(s) for their market research purposes, which may involve sharing your personal data with the relevant client(s). In this context, Kantar is acting as a service provider for its client(s). In any event, you may have the right to restrict the processing of your personal data (see below).

Your personal data collected in market research surveys may be aggregated, anonymized, pseudonymized summarized, and analysed by the Kantar Group global research production teams in the following locations:

- Millward Brown Colombia S.A.S (Colombia, Bogota)
- Kantar EGYPT, LLC (Egypt, Cairo)
- Milward Brown Egypt LLC (Egypt, Cairo)
- Kantar GDC India Private Limited (India, Hyderabad, Pune, Mumbai and Bengaluru)
- Kantar Philippines, Inc (Philippines, Quezon City)
- Kantar GDC Bratislava s.r.o (Slovakia, Bratislava)

To contact us in respect to processing within these Kantar Group locations, please email dataprotection@kantar.com.

Eye-tracking and facial expression data may be collected in some surveys, as described above at the “Lawful Collection and Use of Data” section of this Privacy Notice. Respondents will always be asked for their permission to record this data. This personal data may be analysed, anonymized, and summarized for the aforementioned purposes by Kantar’s analytic partners:

- EYE SQUARE GMBH
  https://www.eye-square.com/en/
  Contact: dataprotection@eye-eye-square.com
  Schlesische Strasse 29-30, D - 10997 Berlin, Germany

- AFFECTIVA INC.
  https://www.affectiva.com/
  Contact: privacy@affectiva.com
  Floor 37, 53 State Street, Boston, MA 02109 United States

Data Transfers

Your personal data may be collected, stored, transferred or processed by companies within the Kantar Group, or third-party service providers for research-related purposes, such as data processing and enrichment, both within and outside your territory. Unless the survey or study requires it, your identity will not in practice be discoverable by the third parties. All parties are contractually bound to keep any information they collect and disclose to us or, we collect and disclose to them, confidential and must protect it with appropriate security standards and practices. If your personal data is transferred to, stored at or otherwise processed outside your country or territory, and that country or territory has not been recognized as providing an adequate level of data protection, we will put in place additional safeguards to protect your personal data, as required by applicable law. For example, if you are in the EEA, standard contractual clauses issued by the European Commission and further appropriate protective measures would be used if we process your data outside the EEA. Where required by law, we will also request your consent for these transfers in accordance with this Privacy Notice and any other necessary information that we provide to you separately.

Where personal information is transferred outside South Africa, Kantar will take reasonable steps to ensure that the recipient is subject to an adequate level of protection through applicable law, contractual safeguards, binding corporate rules, or other appropriate measures, in accordance with POPIA and other applicable data protection laws.

Confidentiality, Security and Industry Requirements

We take appropriate technological and organisational measures to protect your personal data, both during transmission and once we receive it. Our security procedures are consistent with generally accepted standards used to protect personal data. Once we receive your transmission, we will take reasonable steps to ensure our systems are secure.

Measures include security and storage controls that integrate our data and network security policies and procedures with the security requirements of our clients and in line with the requirements of local data protection laws. All Kantar personnel laptops are encrypted, include network protection and storage/processing on removable media/devices is prohibited. Removable media and mobile devices are stored in locked cabinets/drawers/rooms with restricted access together with secure building access. Kantar has also invested in endpoint protection (including anti-malware), threat intelligence, and response services. These measures are deployed across all workstations and servers covering the Kantar estate. Industry/government standard encryption in place - AES128 (Mac) or AES256 (PC), used as standard across the business.

Where possible, and in particular for most of our online surveys, your survey information is anonymised or pseudonymised (by pseudonymised we mean that your identity is disguised so that you cannot be identified without separately-held additional information). Where you have been invited to an online survey by a third-party research panel, technically we may not collect or process any of your personal data because we will not be able to identify you. This is because, in most cases, your identity has been allocated a unique code number that is randomly generated by your panel manager to protect your identity. If you have been invited by a Kantar panel, your survey information is still protected by a code number, and the survey is conducted by a separate part of the Kantar Group of companies. However, in this latter case, your personal information is pseudonymous rather than anonymous and it is still considered and protected as personal data.

Where you have been asked to create an account with us, your account information and personal data are password protected so that you and only you have access to your information. In order to keep your personal data safe, do not divulge your password to anyone. We will never ask you for your password in an unsolicited phone call or in an unsolicited email. Also, please remember to sign out of your account and close your browser window when you have finished visiting our site. This is to ensure that others cannot access your personal data and correspondence if you share a computer

with someone else or are using a computer in a public place like a library or Internet cafe. Please change your password regularly.

In the case of an unfortunate personal data security incident, we will, in a timely manner and in accordance with laws and regulations, inform you of the basic conditions and possible impacts of the security incident, response measures that are already taken or to be taken by us, suggestions for you regarding self-prevention and risk mitigation, our remedial measures for you, etc. We will inform you of such information by email, telephone, or push notification, etc., and when it is difficult to notify each individual affected respondent individually, we will properly and effectively issue a public notice. At the same time, we will also take the initiative to report the handling of personal data security incidents in accordance with regulatory requirements.

Public disclosure

We will only publicly disclose your personal data under the following circumstances:

- After we obtain your explicit consent
- Statutory disclosure: we might publicly disclose your personal data as stipulated by laws, regulations or the mandatory requirements of government agencies

Industry Standards

We adhere to various standards and industry codes (which may depend on the country where we conduct the research), including, but not limited to:

- European Society for Opinion and Market Research (ESOMAR)
- European Pharmaceutical Market Research Association (EphMRA)
- Insights Associations (USA)
- Market Research Society (MRS UK)
- Australian Market and Social Research Society (AMSRS)
- British Healthcare Business Intelligence Association (BHBIA)
- Korea Research Association (Kora)
- Dutch Market Research Association (MOA)
- Intellus Worldwide
- Perhimpunan Riset Pemsaran Indonesia (PERPI)
- Market Research Society of India (MRSI)
- Marketing Opinion And Research Society Philippines (MORES)
- China Marketing Research Association (CMRA)
- Japan Marketing Research Association (JMRA)
- Market Research Society Hong Kong (MRSHK)
- Australian Market and Social Research Organisations (AMSRO)
- Canadian Marketing Association (CMA)
- Advertising Research Foundation (ARF)
- Research Association New Zealand (RANZ)
- New Zealand Industry Code of Practice (Market and Social Research)
- Market Research Society Singapore (MRSS)
- Southern African Marketing Research Association (SAMRA)

Cookie Disclosure

Cookies are small text files stored on your computer or mobile device by a website that assigns a numerical user ID and stores certain information about your online browsing. They are used to help users navigate websites efficiently and perform certain functions. The website sends information to the browser, which then creates a text file on the user’s computer or mobile device. Every time the user goes back to the same website, the browser retrieves and sends this file to the website's server.

When you visit a website or platform for our surveys, we or our clients may use cookies for both necessary purposes (e.g. website functionality and security) and unnecessary purposes (e.g.

marketing). For the latter type, we only do this with your consent. You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly.

For more information, please read the relevant cookies notice/policy on the applicable website or survey platform you have visited and access the cookie preferences page where you are able to adjust your cookie settings.

Cross-context behavioural advertising refers to targeted advertising based on personal information collected from you when you interact with a website or other digital platforms. Except as otherwise described in the applicable cookies notice/policy, we do not provide your personal data to third parties for cross-context behavioural advertising purposes.

Accuracy

We take reasonable steps to keep personal data in our possession or control accurate, complete and current, based on the most recent information made available to us by you and/or by our client.

We rely on you to help us keep your personal data accurate, complete and current by answering our questions honestly. You are responsible for ensuring that you notify us of any changes to your personal data.

Children's Data

We recognise the need to provide further privacy protections with respect to personal data collected from children. We never knowingly invite children under the legal age set by the authorities in the country in which you reside to participate in research studies without appropriate permission. If it is necessary and appropriate to a particular project to directly involve children, we take measures to ensure we have obtained permission from a parent and/or guardian. We will provide parents and/or a guardian information about the survey topic, any personal or sensitive information which may be collected from the children, the way the data will be used and whether and with whom we may share such information.

We do not sell children's personal data and have not done so in the last 12 months. Kantar may collect personal data in collaboration with its client(s) for their market research purposes, which may involve sharing personal data with the relevant client(s). In this context, Kantar is acting as a service provider for its client(s). In any event, individuals (including children) have the right to restrict the processing of their personal data (see below).

Sensitive Personal Data

From time to time, we may collect personal data that is classified as "sensitive" or "special category" personal data. The meaning of this type of personal data varies under data protection laws of different countries. Taking this into account, we treat sensitive personal data as personal data that, if misused or leaked, could potentially endanger an individual's safety, damage their reputation or health, or lead to discriminatory treatment. This includes racial or ethnic origin, citizenship or immigration status, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

In your participation of surveys, you may be asked if you want to provide sensitive personal data. You can always choose whether to provide this data to us. We have included the types of sensitive personal data we ask to collect from you in the above "Lawful Collection and Use of Data" section of this Privacy Notice, including the relevant purpose for processing.

Rights of Individuals

Depending on your location and the data protection laws that apply to Kantar's processing of your personal data, you may have one or more of the following rights in relation to your personal data:

Right	Description
Withdraw consent	The right to change your mind and to withdraw your consent. This will not affect the lawfulness of any processing carried out before you withdraw your consent. It also means that we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.
Access	The right to access copies of your personal data (commonly known as a "data subject access request"). This enables you to request a copy of the personal data we hold about you and to check that we are processing it lawfully.
Rectification / correction	The right to rectify your personal data. This enables you to have any incomplete or inaccurate information we hold about you corrected.
Object	The right to object to the processing of your personal data. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.
Deletion	The right to ask us to delete or remove your personal data where we have no sufficient legitimate reason to continue to process it. You may also wish to exercise this right where you have successfully exercised your right to object to processing or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
Port	The right to port your personal data (portability right). This allows you to transfer your personal data to another party in a portable format.
Restrict processing	The right to restrict processing of your personal data, including your sensitive personal data. This enables you to ask us to suspend the processing of personal data about you — for example, if you want us to establish its accuracy or the reason for processing it.
De-register	The right to de-register from a survey at any time. After de-registration, we will stop providing you with our services and delete your personal data according to our retention policy and your request, unless laws and regulations specify otherwise.
Automated decision-making	Rights in respect to any automated decision-making. If you become subject to automated decision-making, in advance we will provide you with meaningful information about the logic involved, the significance and the envisaged consequences. You also have the right to obtain human intervention, express your own point of view, obtain an explanation of the decision and challenge the decision.

Where our client is the data controller (or equivalent responsible business under applicable data protection laws) for your personal data, we will always co-operate and take instructions from them in respect to your data rights. They may have contacted you separately to inform you of these rights.

Your rights may be limited. For example, if fulfilling your request would reveal personal data about another person, where it would infringe the rights of a third party (including our rights) or if you ask us to delete data which we are required by law to keep or have compelling legitimate interests in

keeping. We will inform you of relevant exemptions we rely upon when responding to any request you make.

If necessary, we shall also notify third parties to whom we have transferred your personal data of any changes that we make on your request. Note that while we communicate to these third parties, we are not responsible for the actions taken by these third parties to answer your request. You may be able to access your personal data held by these third parties and correct, amend or delete it where it is inaccurate.

Accessing Personal Data Rights

To request access to personal data that we hold about you, please see the contact details in the *"How to Contact Us"* section, or alternatively contact our client if they have provided this information to you. When you make a request, you should provide your panellist ID (where applicable) or any other relevant identifiers to the survey, such as the name and date of the relevant survey(s). If you contact us using an email address or contact details for which we do not hold a record of, we may also request you provide a copy of a valid government issued or official identification (such as drivers licence or passport) to verify your request. We do not discriminate against you for exercising any of the rights listed above or any other rights you may have.

You may be entitled to use a third party to submit a request to us on your behalf (sometimes referred to as an 'authorised agent' or similar). For this purpose, we will require proof that you gave that third party signed permission to submit the request, which may be in the form of a power of attorney. We may also require additional verification, such as the identity of the third-party individual.

We aim to respond to your requests to access your personal data rights as soon as possible. However, we will respond within the timeframes determined by the applicable data protection law. Timeframes under data protection laws may be paused whilst we collect essential information from you, such as verification of your identity.

Subject to instructions from our client (where applicable), we will not charge you for your reasonable requests in principle. However, where permissible under application laws, a fee to reflect the cost will be imposed as appropriate on repeated requests beyond reasonable scope. As for repeated requests that are groundless and need excessive technological means (e.g. developing a new system or fundamentally changing the current practices) to fulfil, involve risks to others' legitimate rights and interests or are impractical (e.g. involving information stored on a backup disk), we may reject your request, subject to applicable data protection laws.

Some data protection laws also prevent us from granting your access to your personal data rights, such as where this affects national, defence or public security; major public interests; criminal investigations, prosecutions, trials or enforcement of judicial decisions; the life, property or other important legal rights and interests, or those of other individuals; and trade secrets.

Data Storage and Retention

Personal data shall be retained only for such period as is appropriate for its intended and lawful use, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. Personal data that is no longer required will be disposed of in ways that ensure their confidential nature is not compromised.

Our standard retention period for market research surveys is between 12 and 18 months following completion of the survey, following which your personal data will be deleted or anonymised. However, this can vary in the circumstances, for example if we conduct several related surveys over a longer period of time. If we have collected a video of you for the 'facial expression' purposes detailed above, our partner Affectiva will store this data on our behalf for seven years.

In certain instances, our electronic systems are backed up and archived. These archives are retained for a defined period of time in a strictly controlled environment. Once expired, the data is deleted or anonymised to ensure the personal data is erased. Once anonymised, data you have provided may be used to develop and train artificial intelligence algorithms used for our market research services and products.

Automated Decision-making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making unless we (and/or our client) have a lawful basis for doing so and you have been notified. In such instances, you are also entitled to other related rights (see the "Rights of Individuals" section of this Privacy Notice).

Updates to our Privacy Notice

We keep our Privacy Notice under regular review, and it may be amended from time to time and at least every 12 months. We will always have the most up-to-date Privacy Notice on our website, or within the relevant survey portal. We will record when the Privacy Notice was last revised. Non-material changes to this Privacy Notice will be announced through the relevant website and survey portals only.

How to Contact Us

If you have any questions or concerns relating to your privacy, or if you wish to access your personal data rights or unsubscribe, you can contact Kantar:

- by email at: info@kantar.com
- by post to: The Kantar Group Limited, Vivo Building, 30 Stamford St, London SE1 9LS, or find your local Kantar office location address here: https://www.kantar.com/contact

The Kantar Group Data Protection Officer is Ravinder Roopra who can be contacted as follows:

- Relevant legal entity: The Kantar Group Limited
- Email address: dataprotection@kantar.com
- Postal address: The Kantar Group Limited, Vivo Building, 30 Stamford St, London SE1 9LS

Kantar South Africa (Pty) Ltd has appointed an Information Officer in accordance with POPIA.

Information Officer: Noeraan Hendricks

Email: privacyRSA@kantar.com

Any questions, requests, objections, complaints, requests for correction or deletion of personal information, or requests relating to your rights under POPIA may be directed to the Information Officer using the contact details above.

Additional information regarding requests for access to records held by Kantar South Africa can be found in Kantar South Africa's PAIA Manual, which is available upon request or through the channels specified by Kantar South Africa from time to time.

Complaints

If you consider that our processing of your personal data infringes data protection laws, or you have a related complaint, you may have a legal right to lodge a complaint with a local authority, regulator or supervisory authority responsible for data protection in your country.

However, we would appreciate the opportunity to address your concerns before you do this, so please contact our Kantar South Africa Information Officer in the first instance at privacyRSA@kantar.com or the Kantar Group Data Protection Officer at dataprotection@kantar.com.

If you are located in South Africa and believe that Kantar has processed your personal information unlawfully or infringed your rights under POPIA, you have the right to lodge a complaint with the Information Regulator (South Africa).

Website: www.inforegulator.org.za

General Enquiries: enquiries@inforegulator.org.za

Complaints may be submitted directly to the Information Regulator in accordance with its published procedures.

Kantar South Africa (Pty) Limited a Kantar Group Company.

Our registered name and address are Kantar South Africa (Pty) Limited, 4 Roggebaai Place, Foreshore, Cape Town 8001.

Latest version: Oct 2026