NIPObase

Privacy Notice

Last updated: 2025 11 27 (version 14)

Introduction

This Privacy Notice sets out the commitment of Kantar Netherlands B.V., Amsteldijk 166 Amsterdam and its affiliates Kantar Group companies (altogether “Kantar”, “we”, “our” or “us”), a Kantar Group company ("Kantar"), to the privacy of its panel members (“panellists”, “panellist” or “you”), and governs panellists’ rights regarding privacy and data protection.

This Privacy Notice applies to the NIPObase panel identified in this Privacy Notice as the “panel”. For clarity, this Notice is publicly available on the Kantar website: Privacy (kantar.com).

Panellists are members of the panel, operated by Kantar and for which Kantar is the ‘data controller’, responsible ‘business’ and ‘personal information processor’ for the purposes of applicable data protection law. This means that Kantar is the overarching responsible party for your personal data for the panel, as it determines the purposes and means of the processing of your personal data. For the purposes of this Privacy Notice, ‘personal data’ means any data or information that relates to an identified or identifiable living individual. In certain limited circumstances, Kantar may be acting as a data processor or service provider on behalf of a client for a market research survey. In such circumstances, you will be informed in advance, and it is that client’s responsibility to provide you with information concerning their processing of your personal data.

Taking part in our panel, surveys and research activities is entirely voluntary. By registering to the panel and accepting the relevant terms, 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

Except where you have registered directly with us, we have contacted you to take part in the panel by telephone, post, face to face or online by:

- Receiving your contact information from a third party, such as a research panel or sample provider that you have registered with or been in contact with
- Sourcing your information from publicly available resources
- Or you have previously agreed to be re-contacted by us to possibly participate in further panels or surveys

We collect your personal data in several ways such as: through our website(s) (for example the NIPObase panel 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 Notice.

We have set out more detailed information below 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. These legal bases 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;
- we need to process your data to comply with a legal obligation;
- we need to process your data in order to protect your vital interests or someone else;
- the processing is necessary to perform a task in the public interest; or
- 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).

We will never misrepresent ourselves or what we are doing. 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 Notice.

Case	Purpose	Personal data	Source	Legal basis
Operating our website(s)	Ensure that content from our site is presented effectively, according to the device you are accessing it on. See the "Cookie Disclose" section below for more information.	IP address, operating system information, browser type	We obtain this data from you directly	Legitimate interests to operate our website
Recruitment for the panel	To contact you and invite you to register with the panel and participate in market research surveys (as described further below).	Name, email address, phone number, postal address, other demographic information relevant to a survey (i.e., age, job title, etc.)	We obtain this information directly from you, or from third party recruitment organisations such as research panels or sample providers for which you have opt-in or registered. In limited circumstances, we obtain this information from publicly available sources.	We rely on your consent which has been collected by us or by third parties for this purpose. In limited circumstances, we rely on our legitimate interest to recruit panellists.
Panel registration and management	To administer your panel profile and to communicate with you, including informing you about the panel, selecting you for future surveys, inviting you and contacting you to participate in surveys and other research activities, issuing your incentive, include you in prize draws, helping when you contact our panel support, update, enrich and clean our panel members' data to improve our usage of data, allowing us to better select you for surveys etc.	Name, email address, postal address, mobile device ID, demographics and any detail you share with us about yourself and your household	We obtain this data from you directly. We receive confirmation from our clients that host surveys that you have completed surveys for the purpose of issuing your incentive.	Consent for participation in the panel
Providing you with information	Provide you with information regarding 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.
Market Research	To understand your views about certain products and services or to understand	Identifier, name, email address, voice, image, gender, date of birth, nationality, opinion and	We obtain this data from you directly	Consent when we invite you to participate in a survey

	your behaviour in different situations	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		
Scientific Research for academics, non-profit and charitable research organisations	Including but not limiting to observational studies and studies to gather data about your knowledge and attitude for research and policy purposes	Identifier, contact details, email address, opinions	We obtain this data from you directly	Consent when we invite you to participate in a survey
Safety monitoring (Pharmacovigilance Adverse Events Reporting)	Report Adverse Events during our health studies to our pharmaceutical clients	Identifier, contact details, email address, disease, treatment, product taken and adverse events	We obtain this data from you directly	Consent when we invite you to participate in a survey
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 database	Legal obligation
Security and fraud Protection	Protection of our business interests against fraudulent behaviour and to protect the security and performance of our equipment, property, facilities, personnel, intellectual property, networks, applications and other relevant systems	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 in line with our Terms and Conditions	IP address, browser specifications, device specifications	We obtain this data from you directly	Legitimate interest to ensure the quality of surveys
Tracking of the Answers of Recurring Respondents (special research design projects)	When you participate in our surveys, we typically use a temporary ID which makes your answers in the survey anonymous to our clients. However, some of our clients have the specific research design need to understand how your opinion has evolved over a period of time. For this specific project type that we call "tracking" projects we will use persistent IDs and we will make this clear at the	Persistent unique project-specific identifier	We obtain this data from you directly	Legitimate interests to improve the quality of our data and insights from market research

	beginning of each of these surveys. Your survey responses will be considered as personal data and you will have the right to access them. Such projects will contain a notice on the very first page of the survey, so that you can identify these types of tracking project surveys and decide whether or not to take part.			
Data Matching and Enrichment	We enrich the data we hold about you by matching your personal data with third parties. This will help us to improve your panel 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 database	Legitimate interests to improve the quality of our data and insights from market research
Advertising Targeting and Media Buying Research	We use your personal data to help our clients and data partners enrich their data by using lookalike modelling techniques. Thanks to your participation in our	Persistent unique identifier, contact details, email address, social login, cookie, IP address, mobile device ID, official identification number	We obtain this data from you directly or combined with other secondary database	Legitimate interests to improve the quality of our data and insights from market research

	surveys and your profile data, we can help our clients to improve their advertising targeting, and to create better online advertising models, through lookalike modelling or similar research methodologies. We will use your personal data we collect about you through profile building, participation in research surveys or data matching to match with third-parties and platforms (our data partners). We include contractual safeguards to ensure that you will not automatically be targeted for commercial purposes, as a result of your data being used to help create a lookalike audience, and that our data partners cannot use your data for any other purpose.			
Ad Exposure and Measurement	In addition to cookie-based matching (which you can control and consent to via your panel account), we will use personal data you provide to us, such as an email address, in a direct matching process with third parties (i.e. our clients and publishers) to determine if you are a user of that service (such as social networks, websites, mobile apps) for advertising measurement research purposes. We will identify what advertisements you may have been exposed to on those sites and platforms and measure how brand attitudes or brand recall have impacted sales. The third parties that we work with are not permitted to use the data for any other purpose.	Persistent unique identifier, contact details, email address, social login, cookie, IP address, mobile device ID, official identification number	We obtain this data from you directly or combined with other secondary database	Legitimate interests to improve the quality of our data and insights from market research
Business Transactions	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	Your panel profile, including your name, email address, postal address, mobile device ID, demographics and any detail you share with us about yourself and your household	We obtain this data from you directly	Legitimate interest or where necessary to comply with a legal obligation

Incentives and Rewards

To incentivise you to participate in the panel and market research surveys, we or our clients may reward you with prize draws, vouchers and other incentives. Any incentive program is subject to the applicable terms and conditions of the panel or the relevant survey.

Where we have invited you to participate in a third-party market research survey, we receive confirmation from that third-party where you have completed that survey in order to administer your incentive.

The incentive we offer to you in connection with your submitted information in surveys depends on the amount and type of information you submit and direct us to share with third parties as described in this Notice. If you wish to no longer receive incentives or rewards for your participation, please contact us via the “How to Contact Us” section of this Notice.

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 to perform panel management related activities in order to deliver panel services and activities to you. This could include vendors managing or assisting us in managing our panel databases, marketing automation and CRM, quality checks and fraud prevention, incentive management, and customer care. Some vendors will specifically work with us on enriching your panel profile, 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, name, email address and the information you submit in our market research surveys.

Kantar Group companies and our third-party data partners and publishers 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 may sell your personal data (including your sensitive personal data) to third parties for the participation in surveys and/or other panels from time to time. Before doing so, we will always ask for your consent each time and explain what information is being sold. Where the sale of your information is ongoing, you always have the right to opt-out of the sale and withdraw your consent for future sales of your personal information. Otherwise, we do not sell your personal data (including your sensitive personal data) and have not done so in the last 12 months.]

Your personal data related to the panel may be aggregated, anonymized, summarized, and analysed by the Kantar Group global research production teams in the following locations:

- Kantar GDC India Private Limited (India, Hyderabad, Pune, Mumbai and Bengaluru)

To contact us in respect to processing within these Kantar Group locations, please email us at The Kantar Group Limited email address provided in the ‘How to contact us’ section later in this document.

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. 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 Notice and any other necessary information that we provide to you separately.

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.

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 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, we recommend that you 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 panel 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, fax, telephone, or push notification, etc., and when it is difficult to notify each individual panellist 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 depending on your location, including:

- European Society for Opinion and Market Research (ESOMAR)
- Data & Insights Network (D&IN) (the Netherlands)
- ISO 9001 international standard for quality management systems;
- ISO 20252 international market research quality standard;
- ISO 27001 international standard for data security;
- ISO 14001 international standard for environmental management systems
-

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.

We use cookies for both necessary purposes (i.e., website functionality and security) and unnecessary purposes (i.e., website analytics). 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.

Details of the cookies that we utilise on our website and panel platform are as follows. Click on the name of any third-party Provider to access that parties privacy information.

Cookie Name	Provider	Purpose	Expiry
Panel-session	Kantarmetaskope, (kantarmetaskope.com)	To allow the website to work correctly	48 hours
CSite	Kantarmetaskope, (kantarmetaskope.com)	To allow the website to work correctly	Session duration

If you enter the Kantar NIPObase Portal a functional cookie will be placed on your device to login to this portal.
For more information about the cookies we place and the personal data that may be processed by these cookies, we refer to our Cookie Policy NIPObase.

Cross-context behavioural advertising refers to targeted advertising based on personal information collected from you when you interact with our website or other digital platforms. Except as otherwise described in this Notice and our Cookies Notice on our website, we do not provide your personal data to third parties for cross-context behavioural advertising purposes.

Kantar NIPObase app

When you install the Kantar NIPObase app, we collect the advertisement ID of your smartphone and location data (provided that you enabled this functionality in the app).

The location data is forwarded from the app to our partner Mobidot B.V., which derives movement data from it (such as distance, travel time, means of transport and speed). This location and movement data is analysed by Mobidot B.V. and our partner DAT.mobility B.V. For this analysis we share the following data: panel member ID not traceable to you, gender, age, family size, income category, efficacy, family cycle, education level, urbanity, car ownership and driver's license ownership. As far as relevant for analysing the movement data, we can also share the following data with Mobidot B.V. and DAT.mobility B.V.: other standard background data in our database and data collected in the monthly screening or data collected in surveys as part of the Dutch Movementpanel ("Nederlands Verplaatsingspanel"). After analysing this data we and these parties provide companies and governments an overall insight (so therefore not traceable to you) into the travel behaviour of Dutch people.

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 legal guardian. We will provide parents and/or a legal 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.

While the child is completing the survey, it is the responsibility of the parent and/or guardian to supervise them.

We may sell children's personal data to third parties for the participation in surveys and/or other panels from time to time. Before doing so, we will always ask for parental or guardian consent each time and explain what information is being sold. Where the sale of your information is ongoing, you always have the right to opt-out of the sale and withdraw your consent for future sales of your personal information.

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, 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.

During your time on the panel and 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 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. 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.
Non-discrimination	The right to not be discriminated against for exercising any of the rights available to you under applicable data protection laws.
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.
Complain to a relevant authority	The right to lodge a complaint regarding how process your personal data. See the “Complaints” section below.

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. When you make a request, you should provide your panellist ID or any other relevant identifiers. 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. In some countries, that is one calendar month or 30 days from receipt of the request. Timeframes under data protection laws may be paused whilst we collect essential information from you, such as verification of your identity.

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 fulfill,

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. We shall retain your personal data for as long as you are a member of the panel. In the event that you unsubscribe from the panel, we shall retain data for no longer than 1 month after you unsubscribe, unless otherwise required by law. Personal data that is no longer required shall be disposed of in a manner that ensures that the confidential nature is not compromised.

As part of the Company Business Continuity Plan and as required by ISO 27001, ISO 9001, ISO 20252 and in certain instances the law, 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 and destroyed to ensure the data is erased completely.

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 have a lawful basis for doing so and we have notified you.

Updates to our Privacy Notice

We keep our Privacy Notice under regular review and it may be amended from time to time. We will always have the most up-to-date Notice on our website, or within your panel portal. We will record when the Notice was last revised. Non-material changes to this Privacy Notice will be announced through the panels' sites only.

Original version: 01 November 2016

Latest version: 27 November 2025

How to Contact Us

If you wish to unsubscribe as a NIPObase panel member or have any questions about this, please contact the NIPObase Help Center via

- https://nipobase.zendesk.com/hc/nl

or fill out the contact form via

- https://nipobase.zendesk.com/hc/nl/requests/new.

If you have any questions or comments regarding your privacy or your personal data rights, please contact Kantar:

- by email at privacy.nl@kantar.com
- by post to: NIPObase, PO Box 247, 1000 AE Amsterdam, the Netherlands

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

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 privacy team in the first instance using the details above.

- EU residents can find the contact details of their country supervisory authority via the European Data Protection Board: https://edpb.europa.eu/about-edpb/board/members_en
- You also have the right to complain to the Data Protection Authority. You can direct any complaints about our practices in writing to the Dutch Data Protection Authority ("Autoriteit Persoonsgegevens"), PO Box 93374, 2509 AJ Den Haag, The Netherlands.

- - - - - - - - - - - - - - - - -