

Privacy Policy Healthcare Professional Panel

Last updated: 16/08/2021, version 7

1. Introduction

This privacy policy applies to all members of our Healthcare Professional Panel, which is a respondent database of healthcare professionals managed by us, Kantar Netherlands B.V. (referred to as “Kantar”, “we” or “us”). From time to time we send you invitations to participate in market research surveys.

We are the data controller of the data in our database (e.g. information about your profession, the organisation you work for and your contact details). For the data collected in our surveys, we are the data controller as well, but it could also be our client. Participation in these surveys and providing us with information for our database is entirely voluntary. We ask you to read this privacy policy carefully.

For the purpose of this Privacy Policy, the definition of ‘personal data’ is any information that relates to an identifiable living individual.

2. Lawful Collection and Use of Data

Kantar collects information in several ways from different parts of our site, our mobile application and other activities such as surveys. Examples of these activities are explained below and include:

Registration: some personal data is gathered when you register, such as name, email address, postal address, phone number, information about your profession and the organisation you work for.

Panel Surveys or Research Activities: personal data may also be collected from you when you participate in a survey or in a research activity.

In summary (we’ve provided more details below), the main purposes for which we use your personal data are to:

- Contact you for surveys via email, telephone or any other proposed communication options
- Inform you of updates to our panel services, new features and details relevant to you through panel communications
- Select you for future surveys
- Help you when you contact our support team
- Allow us to reward you with the promised incentives
- Protect us and the Kantar Group from fraudulent behaviour
- Update, enrich and clean our panel members’ data to improve our usage of data
- Evaluate and train our interviewers

We have set out below more detailed information about how we use your personal data. We are also required by law to explain the legal basis for processing your personal data. 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 ‘How to contact us’.

The main purpose for our collecting your personal data is market research. When we contact you, generally by email, by post or telephone we do so to invite you to participate in an online, face-to-face or telephone survey.

Case	Purpose	Data collected/processed
Market Research	To understand your views about certain products and services or to understand your behaviour in different situations	Identifier, contact details, email address, voice, image, opinion
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
Public Disclosure	To share or disclosed 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.
Fraud Protection	Protection of our business interests against fraudulent behaviour.	IP address, browser specifications, device specifications, postal addresses, email addresses, official identification number (i.e. ME number)
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 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 (in the invite or on the very first page of the survey), so that you can identify them and decide whether or not to take part.	Persistent unique project-specific identifier
Survey Participation Uniqueness	Prevention of multiple entries in online surveys by the same individuals.	IP address, browser specifications, device specifications
Quality Control and Training	Evaluating the performance of our interviewers and training them.	Recordings of a telephone interview, contact details
Data Matching and Enrichment	We enrich the data we hold on file about you by matching your personal data with	Persistent unique identifier

	<p>third parties. This will help us to improve your panel profile.</p> <p>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 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 healthcare professionals to create a new user segment). The matching service (our partner) holds the personal data we share for a short time, uses it to assemble the additional information, and then return the combined information to us. Partners are contractually bound to delete the data we share with them or and are not authorised to use it in any way other than for this specific purpose.</p>	
--	--	--

As a member of our Healthcare Professional Panel we may ask you for a range of information, including, for example, your personal opinions, treatment patterns and professional choices. You may decline to answer any questions or withdraw from participation in a study at any time.

3. Third Parties and Data Transfer Across Borders

You can be assured that we will protect your privacy. We will not make your personal data available to anyone without your agreement unless it is for research purposes only or if required by law. This includes your name and e-mail address.

Representatives of our client may watch and/or listen to a qualitative or telephone interview or your contribution on an online platform real time. In advance they will sign a statement in which they promise to keep your personal data confidential. If a representative of our client recognizes you, this person will immediately stop watching and/or listening to the interview or your contribution on the platform. If this isn't possible due to research reasons, we'll inform you about this before you participate in our market research survey.

During a qualitative survey, we will write minutes and make audio and/or video recordings for research purposes. In our survey report to our client we may use quotes from the minutes, parts of the recordings and your platform contribution to illustrate the results of this survey. At our client's request we may also share the minutes, recordings and your contribution on an online platform in their entirety with him. Our client is contractually bound to keep this information confidential and to use it only for internal research purposes.

Your personal data may be collected, stored, transferred or processed by our sister companies within the Kantar group, or third party service providers for research-related purposes, such as data processing, and fulfilment of prize draws or other incentives both within and outside the EEA and the UK. They are all 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 security standards and practices that are equivalent to our own.

If your personal data has been transferred to, stored, or otherwise processed to a territory outside the EEA or the UK (as applicable) and that territory has not been recognised as providing an adequate level of protection of personal data, we will put in place an appropriate legal safeguard. These will include relying on standard contractual clauses approved by the European Commission and other relevant authorities, working with parties that have implemented binding corporate rules or other intra-group processes, obtaining your consent to transfer personal data, where the transfer is necessary for

the performance of a contract between us or where a contract was entered into on your behalf, or where the transfer is necessary to establish, exercise or defend legal claims..

4. Confidentiality, Security and Industry Requirements

We take appropriate technological and organisational measures to protect the personal data submitted to us, both during transmission and once we receive it. Our security procedures are consistent with generally accepted commercial standards used to protect personal data. Unfortunately, no data transmission can be guaranteed to be 100% secure. As a result, while we strive to protect your personal data, we cannot ensure or warrant the security of any information you transmit to us, and you do so at your own risk. Once we receive your transmission, we will take reasonable steps to ensure our systems are secure.

All our employees are contractually obliged to follow our policies and procedures regarding confidentiality, security and privacy.

We adhere to the following standards and industry requirements:

- MOA professional code of conduct;
- ISO 20252 international market research quality standard;
- ISO 9001 international standard for quality management systems;
- ISO 27001 international standard for data security;

5. Cookie Disclosures

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

We do not use cookies on standard online market research surveys.

For behavioural tracking research, we use optional cookies / software applications, but only if you have given your explicit consent to such cookies / applications.

As is true of most online surveys, we gather certain information automatically and store it in survey data files. This information may include things like Internet Protocol addresses (IP address), browser type, Internet service provider (ISP); referring/exit pages, operating system and date/time stamp.

We use this automatically collected information to analyse trends such as browser usage and to administer the site, e.g. to optimise the survey experience depending on your browser type.

6. Accuracy

We take all reasonable steps to keep personal data in our possession or control, which is used on an on-going basis, accurate, complete, current and relevant, 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 and you are responsible for ensuring that the data controller is notified of any changes to your personal data.

7. Rights of Individuals

To request access to personal data that we hold about you, you should submit your request in writing to the e-mail address or postal address shown below in 'How to contact us'.

You have the following rights in relation to your personal data:

- Right to change your mind and to withdraw your consent
- Right to access your personal data
- Right to rectify your personal data

- Right to erase your personal data from our systems, unless we have legitimate interest reasons for continuing to process the information
- Right to port your personal data (portability right)
- Right to restrict processing of your personal data
- Right to object to the processing of your personal data

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.

8. Data Storage and Retention

Personal data will be retained only for such period as is appropriate for its intended and lawful use. In this case we'll retain the personal data in our database till 12 months after resigning your Healthcare Professional Panel membership. We shall retain personal data in our surveys for no longer than 12 months after its use has finalised, unless otherwise required to do so by law. Personal data that is no longer required will be disposed of in ways that ensure their 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 and our affiliates' 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 the physical media destroyed to ensure the data is erased completely.

9. Notification of Material Changes

We keep our privacy policy under regular review and it may be amended from time to time. We will always have the most up-to-date policy on this web page. We will record when the policy was last revised.

Date created: 24/05/2018

Last revised: 16/08/2021

10. How to Contact Us

Questions regarding this policy, complaints about our practices and access requests should be directed to the Fieldwork Team via email at privacy.nl@kantarc.com or in writing to Frank Rem, PO Box 247, 1000 AE Amsterdam, the Netherlands.

You can also contact our Data Protection Officer Ravinderpal Roopra at privacy.nl@kantarc.com. Our Data Protection Officer monitors for instance our compliance with General Data Protection Regulation plus our privacy policy and is our contact point for the supervisory authorities on issues relating to processing personal data.

11. Complaints

We will investigate all complaints and attempt to resolve those that we find are justified. If necessary, we will amend our policies and procedures to ensure that other individuals do not experience the same problem. [Please contact us using the details above.](#)

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.