KANTAR

KANTAR

PRIVACY NOTICE FOR CANDIDATES ("Notice")
Last updated: June 2025

Introduction

This Privacy Notice sets out the commitment of Kantar, and all its affiliate Kantar Group companies (altogether, "Kantar", "we", "our" or "us"), to individuals who apply for a job with, or apply to provide services to, Kantar, or otherwise are registered with us as interested in a potential career at Kantar. This Notice explains how we collect, store and use the personal data you provide before and during any application process. We ask you to read this Notice carefully.

Kantar may update this Notice from time to time, and the latest version of this Privacy Notice is publicly available on the Kantar website at: https://www.kantar.com/privacy-policy-for-candidates.

For the purpose of this Notice, the definition of 'personal data' is information which relates to an identified or identifiable living individual. The data controller or business responsible for your personal data is the Kantar Group entity to which you are applying to or engaging with. In any event, The Kantar Group Limited (registered in the United Kingdom), can be contacted on behalf of your relevant Kantar Group controller / responsible entity – see the 'how to contact us' section below for details.

What personal data does Kantar collect?

The table below describes the categories and types of personal data that Kantar may collect and process about you either during or in connection with any recruitment process (which may vary depending on the role you apply for).

Category of Personal Data	Type of Personal Data
• Contact information	• Name, postal address, personal phone number, personal email address, and emergency contact details.
• Identification information	• Date of birth, passport information, driver's licence or government-issued ID number, national insurance number, immigration status and right to work documentation, nationality,
• Application information	• Candidate details, CV/resume and covering letter, status, current employer, job history, work and corporate title, education, qualifications, references, desired function, salary and work location, licenses, certificates, work experience, business travel information, information obtained from public searches, including social media, and information relating to outside business activities.
• Assessment information	• Assessments and interviews (including automated transcriptions of interviews, manual interview notes, and related scoring of answers by interviewers), aptitude test results and scores, screening and other information collected during the assessment process (including during phone or video calls, emails and other correspondence).
• System information	• Internet login information (including websites visited, applications downloaded, computer IP address, device identifiers and type of operating system and browser type used) as part of any application/candidate portal, information regarding communications sent or received via Kantar's or third party systems, and building access monitoring (including controls for building access, security controls and CCTV footage).
• Any other information you submit to us or we request from you	• Signatures, photographs, opinions, references, your location, and other personal data you provide.

KANTAR

What sensitive personal data does Kantar collect?

Sensitive personal data (sometimes referred to as 'special category' personal data) is defined uniquely under different data protection laws. Taking this into account, at Kantar, sensitive personal data is treated 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.

The table below describes those categories and types of personal data that may be considered as sensitive personal data under relevant data protection laws, and that we may collect or process about you in connection with our recruitment activities.

Category of Sensitive Personal Data	Type of Sensitive Personal Data
• Identification information	• Passport information, driver's licence or government-issued ID number and vehicle licence plate number, national insurance number, immigration status and right to work documentation. • Where required or permitted by law, information related to any background checks.
• Application, System and Network Data	• Account log-in information with any required security or access code, password, or credentials allowing access to a recruitment-related account.
• Equal opportunities related data	• Personal data revealing race or ethnic origin, religious or philosophical beliefs, or data concerning health, sexual orientation, gender identity, or social class/background, only with your consent.
• Reasonable adjustments data	• Data concerning a disability or similar health information you have provided to us to make reasonable adjustments in the recruitment process, to reduce barriers faced by disabled persons.
• Any other information you submit to us or we request from you	• Signatures, photographs, opinions, references, your location, and other sensitive personal data you provide.

When does Kantar collect your personal data?

We collect the personal data referred to above directly from you, from third parties and/or from public sources:

- *From you* – such as through Kantar's websites or its internal or external teams, the application processed or via forms or information you provide in connection with recruitment at Kantar or your job application, including at interviews and assessments or our recruitment events.
- *From affiliated third parties* – such as Kantar clients and colleagues.
- *From unaffiliated third parties* – such as recruiters and employment agencies, websites and job boards, references from third parties, background check providers (subject to the requirements of applicable law), academic institutions, benefits providers (about benefit usage or eligibility), government agencies, certification bodies and other third parties as required or permitted by law.
- From publicly available sources, such as websites, social media platforms and similar channels.

You may be requested to provide the personal data described above as part of the application and recruitment process. If you fail to provide certain personal data when requested, and it is necessary for Kantar to consider that personal data for your application (for example, evidence of your qualifications or work history) or otherwise to comply with our legal or contractual obligations, Kantar will not be able to process your application or continue the recruitment process. In all other cases the provision of your personal data is voluntary.

KANTAR

How does Kantar use your personal data?

This section describes the purposes for which we process 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.

We will only use your personal data for the purpose or purposes for which we collected it, unless we reasonably consider that we need to use it for another reason that is compatible with the original purpose or we have another legal basis to do so.

The table below describes the purposes for which Kantar processes your personal data, and any other personal data you give us or we receive, as well as the legal basis for the use of your personal data.

Purpose of Processing	Legal Basis
• Processing your application and managing the recruitment process. • Assessing your skills, qualifications and suitability for the role including via aptitude tests (as discussed in more detail below), your attendance at an assessment day, and conducting job interviews. • Verifying your identity. • Communicating with you about the recruitment process.	• Where necessary to review and assess your application in order to enter into a contract with you, including pre-contractual steps. • Where necessary for Kantar's legitimate interests and where our interests are not overridden by your data protection rights.
• Keeping records relating to the hiring process. • Conducting business management and financial forecasting. • Maintaining the security of Kantar's facilities, equipment and electronic platforms. • Monitoring compliance with Kantar's protocols and policies. • Taking reasonably necessary steps to ensure Kantar has appropriate and effective health screening measures in place. • Protecting our legitimate business interests and legal rights. This includes use in connection with legal claims, compliance, regulatory, auditing, investigative and disciplinary purposes (including disclosure of personal data in connection with legal process or litigation) and other ethics and compliance reporting tools.	• Where necessary for Kantar's legitimate interests and where our interests are not overridden by your data protection rights.
• Equal opportunities monitoring and/or to provide reasonable adjustments to those with a disability or similar health issue.	• Where necessary for the purposes of carrying out obligations in the field of employment and social security and social protection law under local law. • Where you have given your consent.
• Where required or permitted by applicable law, Kantar may ask you for your consent to carry out certain processing activities, including verification and background checks, and to keep you informed about future job opportunities with Kantar.	• Where you have given your consent to be contacted. • If required or authorised by law to perform background checks.
• Fulfilling our legal obligations to conduct background, screening and eligibility to work checks, where applicable. • Providing a safe working environment for Kantar's employees and other individuals who visit its premises. • Disclosures to law enforcement agencies or in connection with legal claims, health and safety compliance, regulatory, investigative and disciplinary	• Where necessary to comply with a legal obligation.

purposes (including disclosure of personal data in connection with legal process or litigation).	
• 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	• Where necessary to comply with a legal obligation. • Where necessary for Kantar's legitimate interests and where our interests are not overridden by your data protection rights.

How does Kantar use sensitive personal data?

Kantar recognises that sensitive personal data requires a higher level of protection. Under data protection laws, we may often need to have a further justification for collecting, storing and using this type of personal data. We will, if necessary, use sensitive personal data in the following circumstances:

- For equal opportunities monitoring, we will always approach you for your consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware in these circumstances that it is not a condition of your application with us that you agree to any request for consent from us.
- Where necessary for the purposes of carrying out obligations in the field of employment and social security and social protection law under local law.
- For preventing or detecting unlawful acts, where it is necessary and is substantially in the public interest to do so.
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
- Where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

How will Kantar share your personal data?

We collect and process personal data for the purposes described above, but we do not share your personal data to any third parties, unless it is required by law or you have agreed otherwise. We do not sell your personal data (including your sensitive personal data).

Your personal data may be collected, stored, transferred or processed by our sister companies within the Kantar group, or our 3rd party service providers for application-related purposes, such as data processing, both within and outside the UK and the EEA. 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 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 UK or EEA (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. For example, 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, and/or 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).

Confidentiality, security and industry requirements

We have appropriate technological and organisational measures in place to protect your personal data and take all reasonable steps to ensure your personal data is processed securely. Once we receive your data, we will take reasonable steps to ensure our systems are secure. All our third-party contractors, site service providers and employees are contractually obliged to follow our policies and procedures regarding confidentiality, security and privacy.

These 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 also encrypted, include network protection and storage/processing on removable media/devices is prohibited. Removable media 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 is in place (AES128 (Mac) or AES256 (PC)) and used as standard across the business.

Where you have been asked to create an account with us, your account will be password protected so that you and only you have access to your account. 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 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.

Even with the best security, no IT system is completely secure. 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.

Cookies

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 at Kantar, we may use cookies for both necessary purposes (i.e., website functionality and security) and other 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.

For more information, please read the relevant cookies notice/policy on the applicable website or 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 data 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.

Public disclosure

We will only publicly disclose or share 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 or because we have a legal obligation to do so

KANTAR

Accuracy

We take all reasonable steps to keep your personal data accurate, complete, current and relevant, based on the most recent information provided to us. If you would like to update your personal data, please contact us using the details provided below.

We rely on you to help us keep your personal data accurate, complete and current and you are responsible for ensuring that we are notified of any updates or changes to your personal data.

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 the following rights in relation to your personal data:

- Right to change your mind and to withdraw any consent you provided
- Right to access your personal data
- Right to rectify your personal data
- Right to erase your personal data from our systems, unless we have an overriding legitimate interest 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
- Right to limit the use and disclosure of any sensitive personal data in certain circumstances
- Right to de-register from any account or platform you become a subscribed to
- Right to not be discriminated against for exercising any of the rights available to you under applicable data protection laws
- Rights in respect to any automated decision-making in certain circumstances (see the "Automated processing" section below)

You may also have the right to lodge a complaint with your competent data protection regulator (see the "Complaints" section below). However, we would appreciate the opportunity to address your concerns before you do this, so please contact us in the first instance.

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

If necessary, we will notify any other parties such as our suppliers or service providers to whom we have transferred your personal data of any changes that we make when you make a request. Note that while we communicate this to these third parties, we cannot take actions on their behalf. You may, however, 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 below. When you make a request, you should provide details about your relationship with us and any relevant identifiers, such as your name and what role you applied for. 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 applicable 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.

Data storage and retention

Personal data will be retained only for such period as is appropriate for its intended and lawful use, unless we are otherwise required to do so by law. Kantar retains the information collected about applicants until an application decision is made and for a certain period thereafter, unless you have asked us or otherwise agreed to us keeping your information on file so that we can let you know about relevant opportunities in the future. For applicants that are successful, Kantar will retain your personal data as described in our Personnel Privacy Notice. Personal data that is no longer required will be disposed of in ways that ensure their confidential nature is not compromised.

As part of Kantar's Company Business Continuity plan and as required by the ISO 27001, ISO 9001, and ISO 20252 certifications (where held), and in certain instances by 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 the physical media destroyed to ensure the data is erased completely.

Automated processing

In certain circumstances we shall carry out automated processing (including profiling) about you. However, no automated processing will result in any legal or similarly significant decisions being made about you. Any automated processing is merely used to assist a human (i.e. the human will critically review the automated processing before it is used).

If any automated decision made about you is legally or similarly significant and involves no human involvement we will, in advance, provide you with meaningful information about the logic involved, the significance of the decision 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. If you have any questions about this, please contact us.

Use of aptitude tests:

Some of our job applications involve the use of tests, often in the early stages of recruitment, such as psychometric tests, verbal reasoning, and numerical reasoning tests. This is considered a form of profiling, as we may analyse certain aspects of a candidate's personality, behaviour, interests, and habits to help us in our review of their application. The score of any test that you take will be compared to the score obtained by other applicants in your peer group as part of the wider recruitment process. In some cases, these tests may be

processed using artificial intelligence (AI). However, we will never make solely automated decisions about you. In such scenarios, we have implemented various human-in-the-loop safeguards throughout the assessment and scoring process to protect your rights.

In all cases of aptitude testing, we will provide you further information about the tests before you take them, such as what they measure and why that is relevant to your application, how they use your personal data, and what controls that we have in place to mitigate the risks of this technology. We will also provide you with details of any processing using AI tools that we or our suppliers carry out using your personal data.

The answers you submit in aptitude tests, and your test results, are considered your personal data and Kantar is the data controller and responsible party for protecting this data. Kantar relies on its legitimate interests to assess you in the recruitment process as a potential employer. Whilst we do not rely on your consent, you always have the right to raise an objection to Kantar about how we process your personal data, and we will carefully consider whether we have compelling grounds to process your personal data in this way. You will not be discriminated against for exercising this right.

Please note, where we use a third-party aptitude testing platform, they may ask you for additional sensitive personal data to help them ensure their testing is fair and accurate. It is entirely up to you as to whether you wish to provide this information. Kantar will not be informed who provides this, and it has no impact on your application. If you choose to voluntarily provide this to the testing platform, please note that third-party may be the independent controller of that data and will make their privacy notice, which sets out their lawful basis for processing the data, available to you before you complete the test.

You will also be given the option for reasonable adjustments where you suffer from a disability. We will make this option available to you before you take any aptitude test(s) and this will involve you disclosing information concerning your health, which is protected as sensitive personal data. As well as having a legitimate interest as described above, we also rely on our obligation to meet employment and social security and social protection laws as applicable, which includes our obligation to reduce barriers for disabled persons.

Use of Microsoft Copilot (AI):

If you're invited to a job interview, our interviewers may use technology to transcribe the interview, producing a full text record of the conversation. The technology we use at Kantar is called Copilot and is supplied to Kantar by Microsoft, a technology company headquartered in the United States. Copilot is generally considered AI technology as, for example, it operates with a degree of autonomy. You will be given more information about Copilot as an AI system before your interview, where applicable.

After transcribing your interview, Copilot may then be used by the interviewer to organise and structure your answers to interview questions into a document used by the recruitment team to assess and reflect on the interview. Copilot does not score your interview answers or make any decision to hire you, reject you, or move you forward in the recruitment process. Copilot merely will instead organise the sections of the interview transcription into different parts of the review document for information purposes only, to make the recruitment and assessment process more efficient and accurate. All decisions will be made by human recruiters, with consideration as to the risks of AI and automated technology.

The interview transcriptions are considered your personal data and Kantar is the data controller and responsible party for protecting this data. Kantar relies on its legitimate interests to manage the interview process efficiently and accurately. Whilst we do not rely on your consent, you always have the right to raise an objection to Kantar using Copilot in this way and we will carefully consider whether we have compelling grounds to use it. You will not be discriminated against for exercising this right. You can also request copies of your transcription should you wish to see your personal data and consider its accuracy.

KANTAR

Notification of material changes:

We keep this Notice under regular review and it may be amended from time to time. We will record when the Notice was last revised.

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 from any mailing list, 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
- Calling the toll free number +18664711399 (if you are in the United States)

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

New Zealand residents can contact the local Data Protection Officer via email: privacy.nz@kantar.com

China Mainland residents can contact the local Chinese data protection team via email: PIPL-China@Kantar.com

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 at info@kantar.com.

- 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
- UK residents can make complaints to the Information Commissioner's Office via: https://ico.org.uk/make-a-complaint/, by emailing: casework@ico.org.uk, or by post to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
- New Zealand residents can contact the Office of the New Zealand Privacy Commissioner via: https://www.privacy.org.nz/your-rights/making-a-complaint/complaint-self-assessment/, or be email: oia@privacy.org.nz, or be phone: 0800 803 909, or post to PO Box 10 094, Wellington 6143