KANTAR

Data Protection

10 MINUTE READ

Our policy on...

Protecting Personal Data Personally Identifiable Information

First issued: October 2022

Last updated: June 2024

For all Kantar people

Kantar processes data relating to people throughout our business globally. This data can come from our clients, our people, our survey participants, our partners and suppliers. This data is known as personal data or personally identifiable information (PII).

All businesses and organisations are responsible for protecting personal data/PII relating to people. Societies expect these organisations to ensure this people data is protected. It is a position of considerable trust, and the consequences for breaching this trust are significant for both the organisation, and the societies they serve.

The gathering, storage and processing of this personal data/PII is also regulated by national and international data protection privacy laws. Breaching global data protection and privacy laws can have a profound impact on the individual(s) whose data is mishandled. As such, the financial penalties for Kantar can be significant, along with the potential for serious damage to our brand.

We're committed to protecting personal data/PII at all times, and this policy outlines steps you need to take to ensure you work in a way that is compliant.

Any breach of this policy may result in disciplinary action being taken including, in serious cases, potential dismissal or termination of a contingent worker's engagement. This policy is not part of your employment contract or contract for services and Kantar can change or update it from time to time.

01 The Kantar Data Protection Framework

The **Kantar Data Protection Framework** is our "Gold Standard" for processing personal data/PII. It contains detailed data protection policies and processes, and provides you with guidance and tools to enable you to comply with data protection and privacy laws.

It will help you to understand the rules governing your use of personal data/PII at work and who to contact if you need further advice. You can find more information about different data protection and privacy requirements for individual markets on our **Market Specifics** page. Remember, following the Data Protection Framework for each market you are working with will ensure you are always doing the right thing.

02
What is personal data/PII?

Personal data/PII is a broad phrase and covers any information that relates (or can be reasonably linked) to an identified or identifiable living individual. It includes contact details, characteristics, health, race, sex, sexual orientation, opinions (including political opinions), religion, biometrics, trade union membership, market research (including opinions about brands, products and services) and online identifiers, such as cookie IDs, social media handles, device fingerprints and other IDs used for online tracking.

Importantly, information can be personal data/PII even if you do not know the individual's name, email address, phone number or other 'obvious' identifiers.

Sensitive personal data is personal data/PII that, if misused or leaked, could potentially endanger an individual's safety, damage their reputation or health, or lead to discriminatory treatment. This includes personal data revealing an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings.

Any collection or use of sensitive personal data/PII should be strictly controlled and explicit consent must be obtained.

Under data protection legislation, children cannot give consent to allow their data to be collected and processed and you must obtain appropriate permission from a parent or guardian.

03
What are the main sources of personal data/PII at Kantar?

- Emails and attachments
- Databases and/or online systems, cloud storage systems
- Social media or other mass communication tools
- Websites e.g. online employee directories
- Surveys and research data
- CCTV and physical access to sites (e.g. data stored on electronic key cards and location tracking)
- Paper documents such as employee and client contracts, letters, memos, reports, and photographs (e.g. office badges, security passes, employee records)

04
Ten ways you might need to use personal data/PII at Kantar

1. Conducting research and surveys, including media monitoring
2. Compliance with our legal, regulatory and corporate governance obligations
3. Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
4. Ensuring business policies are adhered to (such as policies covering email and internet use)
5. Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking, raising or paying invoices
6. Investigating complaints
7. Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
8. Monitoring staff conduct and disciplinary matters
9. Managing our relationships with our employees
10. Marketing our business

05
How do we protect personal data/PII within Kantar?

Each Kantar Division and Function has an Accountability Lead who is responsible for embedding the Data Protection Framework in their organisation, often supported by Data Protection Champions in each market or team. The Data Protection Champions are the first contact for any queries, followed by the Accountability Lead if the Champion is unable to assist.

Privacy Notices

We must be transparent about the data we collect and use and provide accessible information to individuals about how we will use personal data/PII. This is set out in a privacy notice that we must share with individuals.

All privacy notices must follow the **Kantar's Privacy Notice guidance**.

Data Protection Impact Assessments (DPIA)

Data protection and privacy laws require us to assess the risks associated with collecting and processing personal data/PII in a Data Protection Impact Assessment or **DPIA**. Completing a DPIA will help Kantar collect information the law requires us to hold and ensure we are not using personal data/PII in a way which may cause harm to the individual/s. DPIAs must be completed where there is a high risk to data subjects. The thresholds for this requirement and process for completion are detailed in the **guidance on The Source**. This is vital as DPIAs may be reviewed by relevant authorities in the event of a data incident or investigations.

Data Security

We have implemented technical and operational controls to prevent unauthorised access to Kantar sites and systems. These controls are designed to protect the confidentiality, integrity and availability of Kantar and client information, including personal data/PII.

Data handling and classification

You must always follow **Kantar's Data Handling Guidance** to ensure that personal data/PII is classified and processed appropriately and securely at all times. Once you have determined the classification of the data, you must use the guidance to decide how to process it securely. You must always follow the **Cyber Security for Users policy**.

Minimising personal data/PII

Kantar must not collect irrelevant, inaccurate, or superfluous personal data/PII. Define the business purpose you need the personal data/PII for and only collect sufficient data that is necessary for that purpose. You must then maintain its accuracy and keep it up to date.

Retention and deletion

We must not retain personal data/PII for longer than is necessary. This means that you should not hold personal data/PII longer than required.

Contracts

Kantar must execute written agreements with all our clients, partners, and suppliers to help protect personal data/PII. Please follow the process **here** for contracting.

KANTAR

Our policy on... Data Protection

10 MINUTE READ

How to manage requests from individuals regarding their personal data/PII

Individuals have certain rights in relation to their personal data/PII, including the rights to access information, erasure and to object to how Kantar use personal data/PII.

In the event that you receive a request (also known as a data subject access request (DSAR)), immediately pass the request to **dataprotection@kantar.com**. There are strict time limits (typically 15-30 days) for responding to requests that Kantar must comply with.

How to handle public authority requests

Although rare, public authorities (such as governments, courts and local police) may submit requests to us for the access of information, including personal data/PII. You must not take any further action other than to immediately report any public access request to **dataprotection@kantar.com**.

What to do when something goes wrong

We know that sometimes things may go wrong and personal data/PII may have inadvertently been shared internally or released outside of Kantar, or the Data Handling Guidance has not been followed. If you know, or even suspect this might be the case, you must report this immediately via the Kantar **Data Incident notification** procedure.

You must not disclose any information related to the incident to parties outside of Kantar unless you have been given clearance to do so by the Kantar Data Protection Officer (DPO).

Protecting our:

People | Partners | Integrity | Information | World | Money

06 What training is available?

Our ongoing training and awareness programme creates a culture of effective data protection and privacy compliance.

You must undertake mandatory data protection training when requested.

It is every line manager's responsibility to ensure that their direct reports complete mandatory training.

07 How Kantar maintains its data protection capabilities

We conduct regular internal audits to ensure continual compliance with this policy. In addition, we may have audits from clients and must comply with such exercises where necessary to meet our contractual obligations. Please seek guidance from the central Data Privacy team if a client requests an audit.

08 Key contacts:

Kantar DPO

Kantar central Data Privacy team

If you have any concerns about the way Personal Data / PII is handled within Kantar, and want to raise to them anonymously you can use the **Right to Speak service**.

If you have any questions about this policy, please contact Alison Gallagher, Global Head of Compliance at **businessintegrity@kantar.com**.

If you have any questions about data protection or privacy, please contact the Kantar Data Protection Officer at **dataprotection@kantar.com**.