

Wattle Insights: Data Protection Policy

Date of approval	October 2026
Review date	October 2028
Version	1
Author	Abigail Powell - Director

1. Policy statement

Wattle insights is committed to protecting the privacy, confidentiality, integrity and security of personal data. We comply with the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and other applicable data protection legislation.

This policy sets out how personal data is collected, used, stored, shared and disposed of, and applies to all personal data processed in connection with our business activities.

2. Scope

This policy applies to all personal data processed by Wattle Insights, including information relating to:

- Clients and commissioners
- Research participants
- Workshop and training participants
- Associates and subcontractors
- Suppliers and service providers
- Website users
- Other contacts and stakeholders.

This policy applies to personal data in electronic and paper formats.

3. Definitions

Personal Data

Any information relating to an identified or identifiable living person.

Special Category Data

Personal data requiring additional protection, including information about:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health
- Sexual orientation
- Biometric or genetic data.

Processing

Any operation performed on personal data, including collection, recording, storage, use, disclosure, deletion or destruction.

4. Data Protection Principles

We process personal data in accordance with the following principles:

Lawfulness, Fairness and Transparency

Personal data will be processed lawfully, fairly and transparently.

Purpose Limitation

Personal data will only be collected for specified, explicit and legitimate purposes.

Data Minimisation

We will only collect data that is necessary for the stated purpose.

Accuracy

Reasonable steps will be taken to ensure personal data is accurate and up to date.

Storage Limitation

Personal data will be retained only for as long as necessary.

Integrity and Confidentiality

Appropriate technical and organisational measures will be implemented to protect personal data.

Accountability

We will be able to demonstrate compliance with applicable data protection legislation.

5. Lawful Bases for Processing

We process personal data under one or more of the following lawful bases:

Contract

Where processing is necessary to fulfil a contract or take steps prior to entering a contract.

Legal Obligation

Where processing is required to comply with legal obligations.

Legitimate Interests

Where processing is necessary for our legitimate interests and does not override individuals' rights and freedoms.

Consent

Where individuals have given clear consent for specific processing activities.

Research Purposes

Where processing is carried out for research, evaluation, monitoring or learning purposes in accordance with applicable legislation and ethical requirements.

6. Collection of Personal Data

We may collect personal data through:

- Service contracts and project agreements

- Research activities
- Surveys and questionnaires
- Interviews and focus groups
- Event registration forms
- Website contact forms
- Email correspondence
- Professional networking and stakeholder engagement.

We will inform individuals about:

- Why their data is being collected
- How it will be used
- Who it may be shared with
- How long it will be retained
- Their rights under data protection legislation.

7. Special Category Data

Where special category data is processed, we will:

- Identify a lawful basis and condition for processing
- Collect only what is necessary
- Implement enhanced security measures
- Limit access to authorised persons only
- Obtain consent where required.

Additional care will be taken when undertaking research and evaluation involving sensitive personal information.

8. Information Security

We implement appropriate technical and organisational security measures, including:

Technical Measures

- Password-protected devices
- Multi-factor authentication where available
- Encryption of devices and files where appropriate
- Secure cloud storage services
- Anti-virus and security software
- Regular software updates.

Organisational Measures

- Restricted access to personal data
- Secure sharing procedures
- Confidentiality obligations for associates and subcontractors
- Data protection awareness and good practice.

Paper records containing personal data will be stored securely and disposed of confidentially when no longer required.

9. Data Sharing

Personal data will only be shared where:

- There is a lawful basis for sharing
- The individual has been informed where appropriate
- The sharing is necessary for delivering contracted services
- It is required by law.

We may share personal data with:

- Clients and commissioning organisations
- Professional advisers
- IT and cloud storage providers
- Subcontractors or associates working under contract
- Regulatory or legal bodies where required.

Where third parties process personal data on our behalf, appropriate contractual safeguards will be in place.

10. International Transfers

Where personal data is transferred outside the United Kingdom, we will ensure appropriate safeguards are in place in accordance with UK GDPR requirements. These safeguards may include:

- Adequacy regulations
- International data transfer agreements
- Standard contractual clauses
- Other legally recognised transfer mechanisms.

11. Data Retention

Personal data will be retained only for as long as necessary to fulfil the purpose for which it was collected. Unless contractually required otherwise:

Data Type	Typical Retention Period
Client records	7 years after project completion
Financial records	6 years plus current tax year
Research participant contact details	Until project completion or consent withdrawal
Research data	In accordance with project requirements and ethical commitments
Marketing contacts	Until consent is withdrawn or information becomes outdated

Retention periods may vary depending on contractual, legal, ethical or funder requirements.

At the end of the retention period, data will be securely deleted, anonymised or destroyed.

12. Individual Rights

Individuals have the following rights under UK GDPR:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights relating to automated decision-making and profiling.

Requests relating to these rights should be submitted to the contact identified below.

We will respond within statutory timescales.

13. Data Breaches

Any actual or suspected personal data breach will be:

1. Recorded and assessed promptly.
2. Contained where possible.
3. Investigated to identify cause and impact.
4. Reported to the Information Commissioner's Office (ICO) where required.
5. Communicated to affected individuals where legally necessary.
6. Reviewed to prevent recurrence.

14. Research and Evaluation Activities

In conducting research, evaluation and learning activities, we are committed to:

- Ethical and transparent practice
- Informed consent processes
- Confidentiality and anonymity where promised
- Data minimisation
- Appropriate safeguarding procedures
- Secure storage of research data
- Responsible reporting and dissemination.

Where possible, findings will be reported in aggregated or anonymised form.

15. Responsibilities

The Director of Wattle Insights is responsible for:

- Ensuring compliance with data protection legislation
- Maintaining this policy
- Handling data subject requests
- Managing data breaches
- Reviewing data protection practices regularly.

Any associates, contractors or subcontractors working on behalf of the business are expected to comply with this policy and applicable contractual requirements.

16. Contact Details

For questions regarding this policy or the processing of personal data, contact:

Abigail Powell

Wattle Insights

Email: info@wattleinsights.co.uk

Individuals also have the right to lodge a complaint with the Information Commissioner's Office (ICO):

<https://ico.org.uk>