



Data Protection Policy

1. Introduction

This Policy sets out the obligations of Wizard Pi Ltd, a company registered in United Kingdom under number 09603286, whose registered office is at Unit 5, Offerton Barns, Offerton Lane, Worcestershire, WR3 8SX ("the Company") regarding data protection and the rights of Staff / Clients / Business Contacts ("data subjects") in respect of their personal data under Data Protection Law. "Data Protection Law" means all applicable legislation in force from time to time in the United Kingdom applicable to data protection and privacy including, but not limited to, the UK GDPR, the Data Protection Act 2018 (and regulations made thereunder), and the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation. This Policy sets out the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

2. Definitions

consent means the freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they signify their agreement to the processing of personal data.

data controller means the organisation which determines the purposes and means of processing personal data. The Company is the data controller of all personal data relating to Staff / Clients / Business Contacts used in our business.

- data processor means a natural or legal person or organisation which processes personal data on behalf of a data controller.
- data subject means a living, identified, or identifiable natural person about whom the Company holds personal data.
- EEA means the European Economic Area, consisting of EU Member States, Iceland, Liechtenstein, and Norway.
- personal data means any information relating to an identifiable individual, such as a name, identification number, location data, or online identifier.
- personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- processing means any operation performed on personal data, including collection, storage, retrieval, use, transmission, or deletion.
- pseudonymisation means processing personal data so it cannot be attributed to a specific data subject without additional information, which is kept separately and securely.
- special category personal data means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data.

3. Scope

3.1 The Company is committed not only to the letter of the law but also to its spirit, ensuring lawful and fair handling of all personal data.

3.2 The Company's Data Protection Officer is Joshua Harvey, hi@wizardpi.co.uk. The DPO is responsible for administering this Policy and related procedures.

3.3 All Directors / Heads must ensure compliance by their teams and implement necessary controls and training.

3.4 Any questions relating to this Policy or Data Protection Law must be referred to the DPO, especially regarding lawful bases, consent, retention periods, privacy notices, subject access requests, breaches, security measures, third-party sharing, international transfers, DPIAs, changes in processing purposes, automated processing, and direct marketing.

4. The Data Protection Principles

All personal data must be:

- 4.1 processed lawfully, fairly, and transparently;
- 4.2 collected for specified, explicit, and legitimate purposes and not further processed in incompatible ways;
- 4.3 adequate, relevant, and limited to what is necessary;
- 4.4 accurate and kept up to date;
- 4.5 kept no longer than necessary, unless archived lawfully for public interest or research purposes;
- 4.6 processed securely, with protection against unauthorised processing, loss, or damage.

5. The Rights of Data Subjects

Data subjects have the following rights under the UK GDPR:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure (“to be forgotten”).
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights related to automated decision-making and profiling.

6. Lawful, Fair, and Transparent Data Processing

6.1 Processing is lawful if based on: consent, contract, legal obligation, vital interests, public task, or legitimate interests.

6.2 Special category data requires additional conditions, such as explicit consent, legal obligations in employment/social security, protection of vital interests, non-profit activities, data made public by the subject, legal claims, public health, or research.

7. Consent

Consent must be freely given, informed, and unambiguous.

- It cannot be implied by silence or pre-ticked boxes.
- It must be easy to withdraw at any time.
- Records of consent must be kept.
- If consent is withdrawn, processing must stop immediately unless another lawful basis applies.

8. Specified, Explicit, and Legitimate Purposes

The Company only processes personal data for the specific purposes outlined in Part 24 or as otherwise permitted by law.

9. Adequate, Relevant, and Limited Data Processing

The Company will only collect data necessary for stated purposes. Excessive or unrelated data must not be collected or processed.

10. Accuracy of Data and Keeping Data Up-to-Date

The Company will ensure data is accurate, kept up to date, and rectified or erased promptly if found incorrect.

11. Data Retention

The Company shall not retain data longer than necessary. When data is no longer required, it will be securely deleted or disposed of in line with the Data Retention Policy.

12. Secure Processing

The Company will protect data against unauthorised access, alteration, loss, or destruction, ensuring confidentiality, integrity, and availability.

13. Accountability and Record-Keeping

The Company will:

- Maintain a privacy by design approach.
- Conduct DPIAs where appropriate.
- Provide training to staff.
- Conduct audits.
- Keep records of processing activities, including lawful bases, types of data, transfers, retention, and safeguards.

14. Data Protection Impact Assessments and Privacy by Design

DPIAs will be conducted for new or high-risk processing. Privacy by design principles will always be followed, considering data types, purpose, risks, and mitigation measures.

15. Keeping Data Subjects Informed

Data subjects will be informed of data collection and processing purposes through clear privacy notices. Notices will include company details, purposes, lawful bases, rights, retention, and transfers.

16. Data Subject Access

Data subjects may submit subject access requests at any time via www.wizardpi.co.uk/sar. Responses will normally be provided within one month. Requests are free unless excessive or repetitive.

17. Rectification of Personal Data

Data subjects have the right to request corrections. The Company will act within one month. Where data has been shared with third parties, they will be informed of rectifications.

18. Erasure of Personal Data

Subjects may request deletion where data is no longer necessary, consent is withdrawn, or processing is unlawful. Requests will normally be actioned within one month.

19. Restriction of Personal Data Processing

Subjects may request restriction of processing. The Company will retain minimal data to ensure the restriction is upheld.

20. Data Portability

Data subjects may request their personal data in portable formats. The Company provides data in CSV or Excel. Where feasible, data will be transmitted directly to another controller.

21. Objections to Personal Data Processing

Data subjects may object to processing based on legitimate interests or for direct marketing. Direct marketing objections will always be honoured.

22. Automated Processing, Automated Decision-Making, and Profiling

The Company uses:

- Algorithmic approvals for automated decision-making.
- Segmentation of customers for marketing.
- Data subjects have the right to object, request human intervention, express their viewpoint, and obtain explanations.

23. Direct Marketing

The Company uses personal data for marketing: newsletters, promotional emails, updated service information. Consent is obtained and recorded. Subjects may withdraw consent at any time.

24. Personal Data Collected, Held, and Processed

Data Ref. > Type of Data > Purpose

- WP01 > Company Name > Invoicing / Client Communication
- WP02 > Main Contact. > Client Communication
- WP03 > Email Address > Invoicing / Communication / Marketing
- WP04 > Postal Address > Invoicing / Communication
- WP05 > Alt. Contact > Communication / Marketing

25. Data Security – Transferring Personal Data and Communications

- Emails encrypted with Microsoft 365.
- Emails containing personal data marked “confidential”.
- Secure deletion via System Level Secure Delete.
- Hardcopy transfers via Royal Mail Special Delivery.
- Transmission only over secure networks.

26. Data Security – Storage

- Data stored in encrypted cloud storage.
- Backups taken daily and stored in the cloud.
- No personal data stored on company laptops.
- Data held only in approved platforms: Monday.com, Dropbox, Xero etc

27. Data Security – Disposal

When no longer required, personal data will be securely erased or disposed of in line with the Data Retention Policy.

28. Data Security – Use of Personal Data

- Access requests must be authorised by the Managing Director.
- Transfers must be authorised by the Managing Director.
- Marketing use is the responsibility of the Managing Director / Head of Marketing.

29. Data Security – IT Security

- Passwords must be changed annually and be strong (upper/lowercase, numbers, symbols).
- Security updates installed within 5 working days.
- New software requires approval by the consultant responsible for the device.
- 2FA required for access to personal data systems.

30. Organisational Measures

- Staff trained on data protection responsibilities.
- Annual refresher training required.
- Contractors and agents must comply with the same standards.
- Data sharing only in line with consent and notices.

31. Transferring Personal Data to a Country Outside the UK

Data may only be transferred outside the UK if:

- Adequacy regulations exist;
- Appropriate safeguards are in place (binding corporate rules, SCCs, codes of conduct);
- The subject has given explicit consent;
- It is necessary for a contract, public interest, legal claims, or protection of vital interests.

32. Data Breach Notification

- Breaches must be reported immediately to the DPO.
- ICO notified within 72 hours if rights/freedoms are at risk.
- High-risk breaches notified to affected individuals without delay.
- Notifications include categories and numbers of records/subjects, DPO contact details, consequences, and measures taken.

Approved & Authorised by:

Name: Joshua Harvey
Position: Managing Director
Date: 01/05/2025

hi@
www.

Studio 5, Offerton Barns
Worcestershire, WR3 8SX

wizardpi.co.uk
wizardpi.co.uk