

# Data Protection Policy

---

In the course of our work, we may be required to control and/or process personal information relating to a data subject, which may include employees of our company or other individuals whose data is processed for legitimate business purposes. The European Union General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) set out principles, subject rights, and obligations that we must follow to safeguard the rights and freedoms of these individuals.

We are committed to adhering to the 7 principles of the GDPR and DPA:

1. Lawfulness, Fairness and Transparency
2. Purpose Limitation
3. Data Minimisation
4. Accuracy
5. Storage Limitation
6. Integrity and Confidentiality
7. Accountability

Under the Regulation, data subjects—including employees, customers, partners, and suppliers—have certain rights that we will respect, including:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

In addition to upholding these rights for our staff, we must collectively ensure that the same standards are applied to others, and all employees are expected to handle personal data with the highest level of integrity and confidentiality.

We implement appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage, including access controls, encryption where appropriate, and staff training.

Personal data is retained only for as long as necessary to fulfil the purpose for which it was collected, in accordance with our data retention schedule and any applicable statutory retention periods, after which it is securely deleted or anonymised.

Where personal data is transferred outside the UK or the European Economic Area, we ensure an appropriate safeguard is in place beforehand, such as an adequacy decision or standard contractual clauses, so that the data continues to receive an equivalent level of protection.

Any suspected or actual personal data breach must be reported to the Data Protection Officer immediately. Where a breach is likely to result in a risk to individuals, we will notify the ICO within 72 hours of becoming aware of it and will inform affected individuals without undue delay where the risk to them is high.

Any contravention of the Data Protection Act constitutes a disciplinary offence and will be managed in line with our disciplinary procedures.

We have appointed a Data Protection Officer (DPO) reporting to the Managing Director, who is responsible for:

- Liaising with the Supervisory Authority (ICO) on all matters regarding personal data
- Developing and implementing training and awareness programs for our staff
- Assisting the business to monitor internal compliance, advising on data protection obligations, and providing guidance on Data Protection Impact Assessments (DPIAs)

This policy is reviewed annually, and sooner if required by changes in legislation, guidance from the ICO, or business practice.

Any questions or concerns regarding the interpretation or application of this policy should be directed to the Data Protection Officer and/or the Managing Director.

Signed

*Asim Aziz*

Date

**01/09/2026****Managing Director**