GEM Enterprise

www.gementerprise.uk

Data Protection & Privacy Policy

Date:
January 2026

Introduction and Scope: This Data Protection & Privacy Policy outlines how our company handles personal information in compliance with the UK's data protection laws, including the *Data Protection Act 2018* and the UK General Data Protection Regulation (*UK GDPR*). We are committed to protecting the privacy and rights of individuals (employees, clients, and any other persons) whose personal data we process. This policy applies to all personal data processed by the company, whether it pertains to our customers, website users, employees, or other business contacts, and regardless of whether the data is stored electronically or in paper form. All staff are required to follow this policy to ensure that we handle personal information lawfully and correctly.

Data Controller: GEM Enterprise Ltd (Company No. 08305089), Registered office: 1 Wheatfield Way, Kingston upon Thames, KT1 2TU.

Data protection contact: privacy@gementerprise.uk

ICO registration number: 1

Data Protection Principles: We adhere to the core principles of data processing as set out in the UK GDPR. All personal data handled by the company will be:

- **Processed lawfully, fairly, and transparently:** We will only collect and use personal data if we have a lawful basis (e.g. consent of the individual, performance of a contract, legal obligation, legitimate interest, etc.), and we will be transparent with individuals about how their data is used (typically through privacy notices).
- **Collected for specified, explicit and legitimate purposes:** We will only collect personal information for clear purposes that have been communicated to the individual, and we will not process the data in ways that are incompatible with those purposes.
- **Data minimisation:** We will collect and retain only the personal data that is relevant and necessary for the identified purposes. We will not collect excessive data.
- **Accuracy:** We will take reasonable steps to ensure personal data is accurate and kept up to date. Individuals have the right to have inaccurate or incomplete data corrected.
- **Storage limitation:** We will not keep personal data longer than necessary for the purposes for which it was collected. We will set retention periods for different categories of data, after which data will be securely deleted or anonymised, unless a legitimate reason exists to retain it (such as a legal requirement).
- **Integrity and confidentiality (security):** We will handle data in a manner that ensures appropriate security of personal data. This includes protecting against unauthorised or unlawful access, loss, destruction, or damage by using appropriate technical and organisational security measures (e.g. encryption, access controls, secure storage and transfer protocols).

These six principles guide all our data protection practices. In addition, we recognise an overarching principle of accountability; we are responsible for complying with these principles and must be able to demonstrate our compliance (for example, by maintaining documentation, conducting audits, and implementing policies like this one).

Rights of Individuals: We respect and will uphold the rights that individuals have under data protection law regarding their personal data. These include: the right to be informed about how their data is used, the right of access (individuals can request a copy of data we hold about them), the right to rectification (correction of inaccurate data), the right to erasure (to be forgotten, in certain circumstances), the right to restrict processing, the right to data portability, the right to object to specific processing, and rights related to automated decision-making including profiling. We have procedures in place to receive and respond to individuals'

data protection requests within the required time frames. For example, suppose we receive a subject access request. In that case, we will verify the identity of the requester and provide the requested information or take the appropriate action within one month as required by law. If we decide not to comply with a request, we will provide an explanation to the individual of the reason (along with information on any legal right to complain).

To exercise your rights, contact privacy@gementerprise.uk. If you are dissatisfied with how we handle your data, you can contact the Information Commissioner's Office (ICO). See www.ico.org.uk for contact details.

Lawful Bases and Consent: Whenever we process personal data, we will ensure that we have identified an appropriate lawful basis for that processing as required by the UK GDPR. Depending on the context, the bases we may rely on include: the individual's consent, necessity for a contract we have with the individual, compliance with a legal obligation, protection of vital interests, performance of a public task (unlikely for our private business), or our legitimate interests (balanced against the individual's rights). We will document the lawful basis for each processing activity. Where consent is the basis, we will ensure that the consent is freely given, specific, informed and unambiguous, obtained through a clear affirmative action, and that individuals can withdraw their consent easily at any time. For example, if we use personal data for marketing, we will do so only with consent or under a permissible legitimate interest, and always provide an opt-out.

Data Security Measures: We take the security of personal data very seriously. We implement appropriate technical measures such as password protection, encryption, firewalls, anti-malware software, and secure backup systems to guard against data breaches. Organisational measures are also in place: for instance, we limit access to personal data to only those employees or processors who need it for their job ("need-to-know" basis), and we ensure they are subject to confidentiality obligations. The physical security of our premises (e.g., locked cabinets for paper records) is maintained. We regularly review and update our security measures as needed to respond to evolving threats.

Data Breaches: Despite best efforts, a data breach (unauthorised access, loss or disclosure of personal data) could potentially occur. We have a breach response plan to handle such incidents. Employees are instructed to report any suspected data breach or security incident immediately. In the event of a confirmed personal data breach, we will promptly contain and investigate it. If the breach is likely to result in a risk to the rights and freedoms of individuals (e.g. exposure to fraud or confidentiality breaches), we will notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware, as required by law. If a breach poses a high risk to individuals, we will inform them without undue delay, providing them with information on the nature of the breach and any necessary steps they should take. We will keep records of all breaches, regardless of severity, in order to learn from them and improve our protections.

International Data Transfers: Our business currently does not transfer personal data outside the UK (or outside jurisdictions deemed adequate under UK law). Suppose in the future we need to transfer personal data to a country outside the UK (or outside the European Economic Area). In that case, we will ensure compliance with UK GDPR transfer requirements. This means we will only transfer data if an appropriate safeguard is in place; for example, if the destination country has an adequacy decision from the UK government, or if we have implemented standard contractual clauses or other valid transfer mechanisms. We will also inform individuals if their personal data is to be transferred overseas and the protections in place.

Employee Responsibilities and Training: All employees and contractors who handle personal data on behalf of the company are bound by this policy and are expected to follow data protection procedures. We provide guidance and training to our staff to ensure they understand their responsibilities related to data protection. Employees are reminded to maintain confidentiality and to report any concerns or potential issues (such as someone asking them to share data inappropriately, or noticing a security gap).

Privacy Notices: We maintain clear privacy notices to inform customers, website users, and others about how we use their data. These notices include the types of personal data collected, the purposes of processing, the legal bases, with whom the data may be shared, the data retention periods, and how individuals can exercise their rights or contact us (or our Data Protection Officer, if one is appointed in the future) for more information. For example, our website privacy policy is posted on our website and covers data collected through online forms or cookies.

Monitoring and Compliance: The company's management (or a designated Data Protection lead) will monitor adherence to this policy. We may conduct periodic audits or reviews of data processing activities to ensure compliance and to identify areas for improvement. Non-compliance with this policy by staff could result in disciplinary action, given the importance of data protection.

This Data Protection & Privacy Policy will be reviewed at least annually or whenever significant changes occur in our business practices or relevant law (noting that UK data protection law may evolve). By following this policy, we aim not only to comply with the law but to earn the trust of our customers and contacts by respecting their personal information and privacy at all times.