

## Our Data Protection Commitment

At LoCTA Limited, protecting personal data is central to how we operate. We follow the principles of the EU GDPR and UK GDPR to ensure that your information is handled with care, transparency, and respect.

### GDPR Principles

We are committed to collecting and processing your personal data according to the following principles under the UK GDPR/EU GDPR:

- **Lawfulness, Fairness, and Transparency:** Your data will be processed lawfully and in line with a legal basis under the UK GDPR/EU GDPR, and it will be processed fairly and in a transparent manner.
- **Purpose Limitation:** We will collect and use your personal data only for specified purposes we have informed you about, and we will not further process your data in a manner that is incompatible with those purposes.
- **Data Minimisation:** We will process only personal data that is adequate, relevant, and limited to what is necessary in relation to our purposes.
- **Accuracy:** We will keep your data accurate and up to date.
- **Storage Limitation:** We will keep your data for no longer than is necessary for the purpose for which we process your data.
- **Integrity and Confidentiality:** We will ensure that your personal data is kept secure, and we do this by using appropriate technical and/or organisational measures.
- **Accountability:** We commit to being able to demonstrate that we comply with the above principles in line with our obligations under data protection laws.

### Data Subject Rights

You have certain rights under data protection laws, and we fully support you in exercising them. These include the right to:

- **Access:** Request a copy of the personal data we hold about you.
- **Correction:** Ask us to correct any inaccurate or incomplete data.
- **Deletion (also known as the Right to be Forgotten):** Request that your data be deleted when it is no longer needed.
- **Restriction of Processing:** Ask us to limit the processing of your personal data in certain cases.
- **Data Portability:** Receive your data in a structured, commonly used format or have it transferred to another provider.
- **Objection:** Object to certain processing. You can object to marketing at any time.

For details on how to make a request, please see our [Privacy Notice](#).

When we receive a data subject rights request, we will respond within the required timeframe, provided there are no exemptions limiting us from fulfilling your request.

Where we are the Data Processor of any personal data we will inform the responsible party without undue delay and assist them in their obligations to fulfil such rights requests.

### **Data Breaches**

We take every reasonable step to prevent personal data breaches. However, in the unlikely event that one occurs, we have a clear and tested Data Breach Response Procedure in place.

If a data breach happens:

- We investigate immediately to understand the scope, impact, and root cause.
- We contain and mitigate any risks to individuals and to our systems.
- We document the incident fully in accordance with our internal reporting obligations.
- Where required under the UK GDPR / EU GDPR, we will:
  - Notify the relevant Supervisory Authority within 72 hours of becoming aware of the breach, unless it is unlikely to result in a risk to individuals' rights and freedoms.
  - Notify affected individuals without undue delay if the breach is likely to result in a high risk to their privacy or personal data.

We also conduct post-incident reviews to strengthen our controls and prevent recurrence.

Your trust is important to us, and we are committed to handling all incidents transparently and in compliance with applicable laws.

### **Our Governance & Accountability**

- **Data Protection Officer (DPO):** We have appointed an external DPO to support us with our compliance obligations.
- **Policies & Frameworks:** We maintain internal data protection, information security, and incident response policies.
- **Certifications & Standards:** Cyber Essentials and Cyber Essentials Plus. IASME Cyber Assurance Level 1 and 2 (which map to ISO27001). We align with NCSC Cloud Security Principles.
- **Regular Reviews:** We periodically review our policies, processes, and security measures to ensure they remain effective.

### **How We Protect Your Data**

We apply industry best practices and continuous improvement to keep personal data secure:

- **Privacy Legal Basis:** We review all processing activities to ensure that personal data is processed in a manner that meets UK GDPR/EU GDPR legal basis requirements. This ensures all processing of personal data is lawful.
- **Privacy Notice:** We maintain a privacy notice to provide easily accessible information on how we process personal data.
- **Security by Design & Default:** All of our systems and processes are designed with privacy and security as standard.
- **Technical Measures:** We use encryption, access controls, monitoring, and secure development practices, and implement appropriate technical and organisational measures to ensure a level of security compatible with any risks. We also assess our activities and where required by data protection laws we implement Data Protection Impact Assessments to assess any risks and mitigate these appropriately.

- **Data Breaches & Incidents:** We have breach and incident procedures in place to apply safeguards and effectively manage data breaches through measures that allow us to identify, assess, investigate, and report on these as soon as possible.
- **Retention & Deletion:** We store personal data only for as long as needed to provide our services and meet legal requirements, then securely delete it.
- **Employee Training:** Our staff receive regular training on data protection and information security.
- **Third-Party Management:** We carefully vet service providers who handle data on our behalf, and ensure that the required contractual measures are in place.

### **Contact**

If you have any questions about our privacy programme, please contact us at [privacy@locta.co.uk](mailto:privacy@locta.co.uk)