GDPR

Introduction
The EU General Data Protection Regulation (GDPR) came into effect on the 25th May 2018 across the European Union. GDPR introduces more responsibilities for both data processors and controllers. This includes the need to demonstrate compliance and stricter enforcement, with significant increases to penalties for companies that fail to do so.

This regulation aims to standardise data protection laws and processing across the EU, giving individuals greater say over how, why, where and when their personal information is gathered, processed and disposed of.

Our Commitment
Tiny Tracker is committed to ensuring the security and protection of the personal information that we process. We have always placed a high priority on protecting the data we process, doing so in accordance with accepted industry standards including ISO 27001:2017, however we recognise our obligations in updating and increasing these measures to meet the demands of the GDPR.

Tiny Tracker's commitment to GDPR Compliance has been summarised in this statement and includes procedures, measure and controls to ensure maximum compliance with these new regulations.

How we adhere to GDPR

Information Audit: Carrying out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.

Policies and Procedures: Revising and implementing new data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including:

- **Data Protection:** Our main policy and procedure documents for data protection have been altered to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities.
- **Data Retention and Erasure:** We have updated our retention policy and schedule to ensure that we meet the 'data minimisation' and 'storage limitation' principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new 'Right to erasure' obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.
- **Data Breaches:** Our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.
- **International Data Transfer:** Tiny Tracker only stores data within the EU. Data that is stored in the cloud using Microsoft Azure services, is stored at their UK (West or South) or West Europe data centres.
- **Subject Access Request (SAR):** We have created SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.

- **Legal basis for processing:** We have reviewed all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.
- **Privacy Notice:** We have revised our Privacy Notice to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
- **Obtaining Consent:** We have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.
- **Direct Marketing:** We have revised the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.
- **Processor Agreements:** Where we use any third-party to process personal information on our behalf, we have drafted compliant Processor Agreements and due diligence procedures for ensuring that they (as well as we), meet and understand GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisation measure in place and compliance with the GDPR.
- **Special Categories Data:** Where we obtain and process any special category information (including the data of children), we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special Category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to modify or remove consent being clearly signposted.

Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy access for customers on the Tiny Tracker website, of an individual's right to access any personal information that Tiny Tracker processes about them and to request information about:

- What personal data we hold about them;
- The purposes of the processing;
- The categories of personal data concerned;
- The recipients to whom the personal data has/will be disclosed;
- How long we intend to store your personal data for;
- If we did not collect the data directly from them, information about the source;
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this;
- The right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use;
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances.

Information Security, Technical and Organisational Measures
Tiny Tracker takes the privacy and security of individuals and their personal information very seriously and takes every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction.

Tiny Tracker holds the Certificate of Assurance in compliance with Cyber Essentials Plus and is ISO 27001:2017 certified. This includes several levels of security measures, including:

- All data transfers are done using secure methods (such as SSL for transferring data to and from our web servers).
- Password policies are enforced to ensure any and all passwords meet a minimum level of strength and complexity and are changed regularly.
- Pseudonymisation – Data we store is anonymised after a relevant period of time, to ensure that any sensitive details are not retained for any period longer than they are needed.
- Monitoring is in place for unusual activity, for example attempted access from unrecognised IP addresses, or failed log in attempts.
- Access Control – nobody allowed direct access to database other than the IT support team and the Tiny Tracker system itself.
- All databases are encrypted at rest using AES and 3DES encryption algorithms.
- Firewalls are in place to maximise security.

GDPR Roles and Employees
Tiny Tracker has designated Data Protection Officers and has appointed a data privacy team to develop and implement our roadmap for complying with data protection Regulation. The team are responsible for promoting awareness of the GDPR across the organisation, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures.
If you have any questions about our preparation for the GDPR, your rights, or to submit a SAR please contact Tiny Tracker data protection officer via email at dpo@educater.co.uk