

TPTracker Ltd Data Protection Policy

This document sets out how TPTracker Ltd ensures compliance with all current UK Data Protection legislation, including GDPR.

Data retention

Data files held on individual PCs, laptops or phones: It is TPTracker Ltd's policy not to store any data files containing personal data on any devices other than the TPTracker Ltd server.

Data files held on the TPTracker Ltd server: Each January, any files containing personal data that are more than 12 months old will be deleted. This annual clean-up is scheduled as a recurring event in TPTracker Ltd's diary system and is the responsibility of the Managing Director.

Data files held in TPTracker: Personal data held in TPTracker is owned and controlled by the licensee. The data will remain in TPTracker until the licensee deletes or pseudonymises the data. If the licensee's licence expires, the TPTracker site will be shut down, which will permanently delete all the data held in the site.
TPTracker back-up files: The TPTracker database and all files held in TPTracker are backed up each night. Each backup is retained for one month and then over-written with a newer backup, permanently destroying the older copy.

Paper documents: It is TPTracker Ltd's policy not to store any documents containing personal data for longer than 3 months. All such documents will be disposed of using a 3rd Party, on-site, secure, data shredding contractor who provides a written record.

TPTracker databases

These are databases belonging to and supplied by TPTracker licensees, which may include personal data. TPTracker Ltd will never act as the Data Controller, only as the Data Processor, with respect to these databases.

The role of TPTracker Ltd as Data Processor will be as defined in a written contract with each TPTracker licensee or, in the absence of a specific contract, as defined in TPTracker Ltd's "Information Sheet 3: Data Protection".

It is TPTracker Ltd's policy to only hold copies of these databases in TPTracker. They will not be stored on individual devices. They will only be stored on the TPTracker Ltd server when the Data Controller has instructed TPTracker Ltd to conduct some analysis or processing of the data; such files will be subject to the Data Retention Policy detailed above.

TPTracker Users

TPTracker Ltd will only hold the personal details of TPTracker users in TPTracker; this will comprise Name, Job title, Group, Landlord, Email, Telephone number and Role.

TPTracker Ltd will hold the details above to enable us to:

- Manage the user's authorised access to TPTracker;
- Inform the user of any changes to TPTracker access and functionality which may affect them;
- Advise the user of any TPTracker training, workshops and networking events which may interest them.

TPTracker Ltd will not share the user's contact details with anyone else, without asking the user first and receiving confirmation from them by email.

As soon as a person is deleted from the list of registered TPTracker users, TPTracker will automatically and permanently delete their personal details. Any records created in TPTracker modules which refer to them by name may remain, but will not be linked to their personal data.

Users are required to accept these terms if they wish to be a registered user of TPTracker.

Passwords and secure login details are only given face to face or by telephone when the identity of the recipient has been confirmed; they are never sent by email or post.

TPTracker data transfers

TPTracker Ltd will only transfer data files containing personal data (a) with the permission of the Data Controller and (b) by means of a secure link.

The secure options available are:

- Via TPTracker;
- Via a secure FTP site;
- Via email, only if the data file has been password protected.

TPTracker sub-contractors

The relationship between TPTracker Ltd and a sub-contractor who may have access to personal data, will be governed by a written contract covering:

- The means of transferring data securely to the sub-contractor;
- The secure storage of that data while it is held by the sub-contractor;
- The authorised use of the data;
- The retention and secure disposal of the data;
- Staff training and vetting;
- Notification of any breaches in procedure.

TPTracker Ltd marketing contacts

TPTracker Ltd will only respond to specific requests for information on an individual basis; we will never send out unsolicited communications.

TPTracker Ltd will only hold the personal details of marketing contacts who have requested us to do so and for as long as they wish to remain in contact.

Staff training

Each member of the TPTracker Ltd team will be thoroughly briefed on current UK data protection regulations and be able to advise our customers on these requirements.

Each member of the TPTracker Ltd team will be required to study this document and sign a copy to confirm that they have done so and will follow its procedures.

The TPTracker Ltd Data Protection Policy will be reviewed and re-signed annually.

A breach of this policy is treated as a serious disciplinary offence in the TPTracker Ltd Disciplinary Code.

Breach notification

Every suggestion of a possible breach of data security will be logged immediately in the TPTracker Ltd Data Breach log. The record will include the date and time the incident was identified, the scope of the incident and the nature of the suspected breach.

Each entry in the log will be evaluated immediately by two senior members of staff, to decide if a breach has indeed occurred.

If a breach is believed to have occurred, the client (Data Controller of the relevant data) must be informed at the earliest possible opportunity.

The Data Controller and TPTracker Ltd will agree (and record by exchange of emails) which party is to inform the ICO. The ICO must be informed within 72 hours of the suspected breach.

Thereafter, a full and thorough investigation of the incident must be conducted jointly with the client and if appropriate any relevant sub-contractor.

Updated 01.05.23