Data Protection and Data Security Policy

This policy sets out Threemo's commitment to protecting personal data under the General Data Protection Regulations (GDPR) and how we will implement that commitment in our role as data controller.

Any queries relating to this policy should be sent to the Data Protection Officer, Hayley Masheder : hayley@threemo.co.uk

Our commitment

Threemo is a data controller, this means that we determine the purposes for which and the manner in which, your personal data is processed. As a data controller, Threemo is committed to:

- Ensuring personal data is processed fairly and according to legally compliant standards of data protection and data security;
- Ensuring personal data is processed only for the specified and lawful purpose;
- Taking steps to ensure personal data is adequate and relevant to the purpose(s) for which they are being processed;
- Taking steps to ensure personal data is accurate and up to date;
- Ensuring personal data is only retained for a necessary period;
- Providing individuals with access to their data;
- Providing adequate security measures to protect personal data;
- Ensuring a nominated officer is responsible for data protection compliance;
- Providing adequate training for all staff responsible for handling personal data;
- Regularly reviewing data protection policies and guidelines.

We are committed to ensuring that we comply with the data protection principles of GDPR as outlined at the end of this policy and we will protect personal data in the following ways:

1. Collecting personal data

   Personal data may be processed as necessary to perform a contract with the data subject and our privacy notice explains what personal data we are gathering and for what purpose(s).

   We will only collect personal data that is necessary for the purpose(s) declared.

   We will obtain the appropriate consent where it is required.

2. Safeguarding personal data

   Data will not be kept longer than is needed and we will take all reasonable steps to delete information when we no longer need it. The periods for which we hold personal data are contained in our privacy notice.

   Threemo will use appropriate technical and organisational measures to keep personal data secure and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Maintaining data security means making sure that:

a. only people who are authorised to use the information can access it;

b. where possible, personal data is encrypted;

c. information is accurate and suitable for the purpose for which it is processed;

d. authorised persons can access information if they need it for authorised purposes;

e. Any desk or cupboard containing confidential information must be kept locked;

f. Computers should be locked with a strong password that is changed regularly or shut down when they are left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others;

g. Data should never be stored on CDs or memory sticks;

h. The Data Protection Officer must approve any cloud used to store data;

i. Data should never be saved directly to mobile devices such as laptops, tablets or smartphones;

j. All servers containing sensitive personal data must be approved and protected by security software;

k. Servers containing personal data must be kept in a secure location;

l. Data should be regularly backed up in line;

m. Particular care must be taken to avoid inappropriate disclosures over the telephone and thus the identity of any telephone caller must be verified in line with internal procedures before any personal information is disclosed. If the caller's identity cannot be verified satisfactorily then they should be asked to put their query in writing.

n. Paper documents should be shredded.

Where data has been destroyed, appropriate measures are taken to ensure that the data cannot be reconstructed and processed by third parties. Adequate measures are taken to safeguard data to minimise the risk of loss, destruction or unauthorised disclosure.

Threemo employees will not disclose any information about an individual to a third party unless they are clear they have the appropriate authority to do so. Personal data will not be disclosed to public authorities unless authorised by the Data Protection Officer or Nominated Officer.

Any ‘personal data breach’ by Threemo staff will be treated seriously and may lead to disciplinary action, up to, and including dismissal.

If individuals consider that any information held about them is inaccurate or out of date, then they should tell the Data Protection Officer. If they agree that the information is inaccurate or out of date, then they will correct it promptly. If they do not agree with the correction, then they will note the comments.

3. Processing personal data – Management Information Systems used to obtain and process personal data are reviewed to ensure they are as secure as possible. Ongoing due diligence is undertaken against any third party who processes data on our behalf. Personal data will not be processed except for the purpose(s) for which they were collected. We will obtain consent from the individual to process their personal data if the purpose changes.

Data access

Individuals have extended rights over their data under GDPR. These include the right to object to their data being processed and the right to have their personal data deleted or transferred in some circumstances. We will not transfer or disclose personal data to any third parties except in line with our Privacy Notice, as required to fulfil our contractual obligations with the individual or as is required by law.

Individuals have a right to access their personal data and can request the information by completing our Subject Access Request Form and Guidance For Our Clients. The individual will also need to submit supporting documentation to establish their identity and confirm the data refers to them.

The request will be determined by or with the authority of the Data Protection Officer.

Data breaches

If we discover that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner's Office within 72 hours of discovery.

Thremo will record all data breaches in our Data Breach Log regardless of their effect in accordance with our Data Breach Notification Procedure.

If the breach is likely to result in a high risk to an individual's rights and freedoms, we will tell affected individuals that there has been a breach and provide them with more information about its likely consequences and the mitigation measures it has taken.

Training

We will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy will receive additional training to help them understand their duties and how to comply with them.

The GDPR Data Protection Principles

Article 5 GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.