

Data Protection Policy for Clients

1. Policy Statement

The protection of personal data is governed within the UK and European Union by a legal framework called the General Data Protection Regulations (GDPR). Eastwood & Partners (Consulting Engineers) Limited act as both a data controller and processor and are committed to ensuring that we are compliant with GDPR by keeping personal data safe, secure, confidential, and only using it for legitimate business purposes. We are also registered with the Information Commissioners Office (ICO).

2. Purpose of the Policy

It is the purpose of this policy to demonstrate to our clients how their personal data and their client's personal data are kept safe, secure and confidential.

This policy will also outline how we handle, store and process personal data, including the measures we take to ensure that all personal data is stored and processed securely. It is our aim, in conjunction with this policy; that our clients will understand how Eastwood & Partners legally collect, process and store their personal information.

3. Processing and Controlling Personal Data

Personal Data is any information relating to a living person who can be identified directly or indirectly by the data, including any expression of opinion about that individual.

We are Processors: Eastwood & Partners are given personal details (name, address and contact details) and act as a processor of personal data to enable us to deliver services to our clients. In situations where we act as a processor of personal data, we will use it and store it strictly in accordance with GDPR regulations. We will expect clients who have shared the personal data with us to also have a legal basis for holding the data or obtained consent, if required.

We are Controllers: Eastwood and Partners also obtain personal data directly from clients acting as controller to enable us to deliver our services to a client directly. When we are given personal data directly from a client our legal reason for processing this personal data is normally that we have a contract in place with a client and we need to process the

personal data to comply with our obligations under the contract. We do not therefore directly ask for consent, due to our legal basis.

4. The Storage of Personal Data

Eastwood & Partners has an electronic project filing system where data is securely stored in individual electronic project files. These files are can only be accessed by authorised individuals who have a legitimate reason to have access, namely the Engineers and staff at Eastwood and Partners.

Personal Data can also be held on an electronic project management software platform (PMS). Our PMS typically contains names, addresses and contact details of our clients and enables us to quickly access personal data for business reasons. Our PMS enables us to comply with our obligations under the contract with a client in an efficient and timely way, delivering a more effective service to our client base.

5. Sharing Personal Data

Your personal data will not normally be shared with any third parties other than those software platforms outlined above. We engage an IT support consultancy and accountancy firm who could have access to personal data as and when they work alongside us to maintain our systems. We have carried out the necessary checks with these software platforms and third parties to ensure GDPR compliance and to confirm that your personal data is secure, and not shared.

Although it would be unusual, if we do have to share personal data with a third party to meet our obligations under the contract with a client, we will ensure that they are aware of their obligations under the GDPR. On completion of the contract, we expect all our clients (where legally able) to delete any personal data they store.

6. The Security of IT Systems

Our computer systems run a layered security system, which is the practice of combining multiple mitigating security controls to protect resources and data. We have our perimeter defences tested as part of our Cyber Security Essentials membership. Computer security testing is conducted annually. Access to any data on our system is restricted by job function which is reviewed on a regular basis.

All data stored on network drives is securely backed up locations. Our backups exceed best practise guidelines and recovery is tested regularly. We encrypt all HR data that is backed up offsite. Access to our data by support organisations is also covered under the GDPR and their policies have also been confirmed to be in compliance.

All staff at Eastwood and Partners use passwords to access our IT systems and these have been created by our IT department to maximise security. These passwords are regularly reviewed and staff cannot change their own passwords. We also educate all our staff on cyber security and safe practices when using e-mail and IT systems. This is to reduce the risk of a cyber-attack which may compromise the security of personal data stored on our systems.

7. Retaining your Personal Data

We only retain personal data relating to projects due to legal and statutory reasons and we comply with GDPR on the retention of data. We aim to delete all personal data which will not be required for statutory or litigation reasons within the recommend framework.

8. Data Subjects Rights

The GDPR provides individuals or data subjects with a number of rights which we have outlined below. We ask all our clients to be aware of these (or their) rights and ensure that they also communicate these to any individuals whose personal data they ask us to process.

- **Transparency:** We encourage compliance and transparency when it comes to the storage and processing of personal data and therefore in addition to this policy we have appointed a Data Protection Officer (DPO), Terry Carlin (IT Manager). The DPO can and will assist and advise individuals and Eastwood & Partners on compliance with the GDPR and provide a point of contact for employees (and ex-employees) if they wish to discuss the legitimate use, storage and processing of their personal data.
- **Raising a Concern (Data Breaches):** Clients should raise any concerns of data breaches or unlawful processing of personal data with a Director or the Data Protection Officer immediately and without delay. Any validated data breaches will reportable to the ICO (Information Commissioners Office) and individual's (data subjects) will be informed if affected.

- **Subject Access Requests:** Individuals can request a copy of their personal data. This is called a Subject Access Request. The request must be in writing to a Director or the DPO with sufficient detail to enable us to identify the data requested. Once sufficient detail has been obtained, the data will be provided within a 40 day period and will be free of charge. Multiple or repeat requests may be subject to an administration charge if a legitimate reason for a repeat request is not given.
- **The Right to be Forgotten:** Individuals have the right to be forgotten and therefore can specifically request for their personal data to be deleted. We will consider their request where there is no compelling or statutory reason to retain information. If you wish to remove your personal data from our records, please raise this with a Director or the Data Protection Officer in writing and we will discuss this with you. Please note we may be legally required to retain some information as outlined in point seven of this policy.

9. Further Information on Information Commissioners Office

The ICO is the UK's independent body set up to uphold information rights and govern compliance with data protection laws, namely the GDPR. They are also the body to which unlawful data breaches can be reported and investigated and they have the authority to issue penalty fines for breaches. The ICO will assist individuals in understanding their rights regarding personal information. For more information, please visit www.ico.org.uk.