

TEKMAR GROUP

PRIVACY POLICY & PROCEDURES

OVERVIEW

We take our obligations under privacy and data protection law seriously. This Privacy Policy sets out how we deal with the personal information we collect, why we use it and how we protect it.

Within **Tekmar Group Plc** and all subsidiaries (*hereinafter referred to as the “Company”*) we collect personal information to effectively carry out our everyday business functions and activities and to provide the products and services defined by our business type. Such data is collected from employees, customers, suppliers and clients and includes (*but is not limited to*), name, address, email address, date of birth, IP address, identification numbers, private and confidential information, sensitive information and bank details.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to processing all personal information in accordance with the **General Data Protection Regulation (GDPR)**, **UK data protection laws** and any other relevant data protection laws and codes of conduct (*herein collectively referred to as “the data protection laws”*).

The Company is registered as a data controller with the Information Commissioner’s Office, which is the UK’s independent body set up to uphold information rights. As a data controller we are responsible for ensuring that when we process personal information we comply with data protection laws.

This policy applies to all staff within the Company (*meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, and agents engaged with the Company in the UK or overseas*). **Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.**

KEY TERMS
Personal information also referred to as ‘personal data’ and means information about a living individual who can be identified from that data. Some of the information will identify the individual directly, perhaps by reference to a name and email address. It is also possible to identify an individual when a name isn’t used, for example, by their job title and employer, or by an online identifier such as an IP address.
Sensitive personal data includes information about an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sex life or sexual orientation, or about any offence committed or alleged to have been committed by that individual.

OBJECTIVES

We are committed to ensuring that all personal information processed by the Company is done so in accordance with the data protection laws and its principles and we will process personal information to comply with the eight principles of good practice. Personal information must be:

- Processed fairly and lawfully
- Processed for limited purposes and in an appropriate way
- Adequate, relevant and not excessive for the purpose
- Accurate

- Not kept longer than necessary for the purpose
- Processed in line with individuals' rights
- Secure
- Not transferred to people or organisations situated in countries without adequate protection

THE PERSONAL INFORMATION WE COLLECT

We collect personal information in the natural course of our business activities. Under data protection law we can only use personal information where we have a proper reason for doing so, which includes:

- complying with our legal and regulatory obligations
- for our legitimate business interests
- for the performance of our legal agreement with you
- where you have given consent

The table below sets out the main areas of personal information we collect, and what we use this information for:

Personal information we will / may collect	What we use this for
Employment: Your name, address and contact details Information to enable us to check and verify your identity, eg. your date of birth or passport details Information for employment purposes, eg. national insurance number and bank account details Correspondence including <ul style="list-style-type: none"> - Contract of employment - Correspondence eg. re pay rise or change of role - Emergency contact details - Holiday sickness and other absences - Appraisals and training records 	Payroll processing To meet employment regulations To comply with our health and safety and occupational health obligations
Information Technology: Use of IT systems, eg. use of business systems, IP address, browser and operating systems Communication methods, eg. leaving a voicemail message	To support efficient business processes To maintain IT security and secure infrastructure
Contractual requirements: Individual contact details provided in the course of doing business	To support the performance of our contractual obligations
Marketing information: Your name, address and contact details Information you provide us, eg. by completing our business surveys Marketing preferences, eg. when you subscribe to our website for updates	To communicate with the business community in which we operate To support the growth and success of our business
Security: Building security, eg signing-in registers, door access systems, CCTV monitoring	To comply with health and safety regulations To maintain security in and around the premises to protect personnel and property

This is not an exhaustive list and we may collect other personal information not listed above and we will ensure it complies with our Objectives (2.).

WHO WE SHARE PERSONAL INFORMATION WITH

We share personal information with:

- Professional advisors including auditors, tax advisors, lawyers
- IT support and service providers
- External service providers, such as our payroll bureau
- Our bank
- Marketing host services

We only allow third parties to handle personal information where we are satisfied that their processes will protect this information.

Personal Information is held at our offices and by those third parties we authorise to do so, and it is held in securely to ensure the appropriate level of confidentiality is applied.

TRANSFERRING INFORMATION OUTSIDE THE EUROPEAN ECONOMIC AREA

Sometimes we may need to share some personal information outside the European Economic Area (EEA) eg:

- with our agents or representatives with offices outside the EEA
- with our customers or suppliers located outside the EEA eg. employee details to be sent in advance to obtain security clearance at a customer's site

Such transfers are subject to special rules and we will undertake an assessment of the level of protection required for the details surrounding the transfer. We will minimise the information transfer and may need to seek consent from the individual in the circumstances.

HOW LONG WILL PERSONAL INFORMATION BE KEPT

We will only keep personal information for as long as is necessary to fulfil the purposes we collected it for, including satisfying legal accounting and/or reporting requirements. We have assessed the areas across the business where personal data is collected and evaluated the envisaged time limit for each category of data. We will take all reasonable steps to delete or anonymise all personal information which is no longer required based on this evaluation, and in line with those retention periods set out by law.

DATA SECURITY

We will take appropriate security measures against unlawful or unauthorised processing of personal information, and against its accidental loss or damage too. We will use appropriate IT security measures to protect information held electronically, particularly on portable devices such as laptops and mobile phones eg. Encryption software.

We will maintain data security by protecting the confidentiality, integrity and availability (for authorised purposes) of the personal data.

PROCESSING IN LINE WITH YOUR RIGHTS

We will process personal information in line with your rights, in particular your right to:

- Request access to personal data we hold about you
- Prevent the processing of your data for direct-marketing purposes

- Ask to have inaccurate data amended
- Prevent processing that is likely to cause damage or distress to yourself or anyone else
- Object to any decision that significantly affects you being taken solely by a computer or other automated process

You are entitled at any time to ask us for a copy of the personal information we hold about you – see Contact Information. Information will be provided to the individual at the earliest convenience, but at a maximum of 30 days from the date the request is received.

CONTACT US

We will regularly monitor and assess the collection of personal information to ensure compliance to this policy. If you are aware of any non-compliance or wish to raise a query or complaint, please contact:

Lynn Hood on 01325 379520
or at lynnhood@tekmar.co.uk