GDPR
POLICY

Introduction

The General Data Protection Regulation [GDPR] came into force in May 2018. This puts onerous responsibilities on both us as employers and on you as employees. It requires that we ensure that data collected is fairly and lawfully processed and that any information we hold relating to a Data Subject is adequate, relevant and not excessive. Personal data relates to individuals whether those individuals are customers or suppliers, prospects, employees of customers or suppliers or our own employees.

This concise data protection policy statement aims to give sufficient information to all employees to ensure that they have an adequate understanding of the legislation to comply with it. A full Data Protection Policy will be issued to all managers/heads of department and is available to anyone who requests it.

Employees should be aware that it is a criminal offence to access or disclose personal data held without authority. Misuse of data will be dealt with in accordance with the disciplinary procedure. As part of your contract of employment, and by signing, you have consented to us holding and using personal data relating to you.

What Information is included?

Personal data means anything about an identifiable individual including, for example, names and addresses, bank details, health records and most of the information that we need to hold about you for employment purposes. The majority of information that we hold is required on a legal basis or for the legitimate interests of the company. Where the data processing activity is not obvious you will be informed.

Where data is given by one party directly to another the person giving the information gives consent to use the data for any legitimate business purpose. However, everybody must be aware that passing on information to other parties without the consent of the data subject could put them in breach of the regulation. This includes forwarding e-mails, passing on phone numbers etc.

Responsibilities

All employees have a responsibility to ensure that: -

- Personal data is not held or used otherwise than for the legitimate business interests of the company.
- Appropriate measures are implemented to protect the data; see the Electronic Media Policy for further information.
- Those authorised to access data have the responsibility to protect it.
- Data is not disclosed to third parties unless there is a legitimate business need or without the data subjects consent.
- Inform the relevant departments of any changes to your personal data at the earliest opportunity.

Data subject's rights

- All queries relating to data control should be addressed to Mike Roberts and can be made during normal hours of work via e-mail or at any time by letter.
- You have the right of access to the data held about you and we will ensure you receive it within 30 days of any request.
- You have the right to request rectification, erasure or restricted processing of data held about you.
- We will take any request seriously and comply with it providing that we are able to do so without compromising the legitimate business needs of the company. All requests will be responded to in compliance with current legislation.
- Employees have the right to complaint to the Information Security Officer ICO (Mike Roberts) if they think there is a problem with the way we handle data.

Breach

In the event of a breach of protection of personal data, you must report the matter ICO or in their absence to another company director. A procedure will be implemented to limit the consequences, report the breach to those required, investigate the breach and ensure that action is taken to prevent reoccurrence.

This policy shall be reviewed for its effectiveness and suitability at least annually as part of the Management Review process.

Signed:
Mike Roberts
Managing Director
Watermark Systems (UK) Ltd

Date: 6th January 2022