Data Protection Policy

Document Number:	ATP004	Revision:	1
Issue Date:	17/01/2022	Complied by:	Alex Mountain
Review Date:	18/01/2025	Reviewed/Authorised by:	Peter King

Revision	Date	Change(s)
1	17/01/2022	Document reviewed

Introduction

The General Data Protection Regulation (GDPR), as supplemented by the Data Protection Act DPA 2018 (DPA), is the main piece of legislation that governs how AccessTec Ltd collects and processes personal data (references hereafter to "AccessTec" or "the Company" mean AccessTec Ltd). AccessTec is fully committed to compliance with all legal requirements regarding data protection because the Company understand that failure to comply with this legislation may have severe consequences.

The legislation applies to anyone processing personal data. It sets out principles which should be followed and gives rights to those whose data is being processed. To this end, AccessTec fully endorses the eight principles of data protection. The data we collect is:

1. Processed fairly and lawfully
2. Only to be obtained for specified and lawful purposes
3. Relevant, and not excessive
4. Accurate and up to date
5. Not kept for longer than necessary
6. Processed in accordance with the subject's rights
7. Kept securely
8. Not to be transferred to any other country without adequate protection in place

Personal Data Relating to Employees

Throughout employment and for as long as is necessary after the termination of employment, AccessTec will need to process data about employees. We ask at the beginning of employment for the employee to agree to personal data being held and processed, a copy of the document that is signed will be available. The kind of data that AccessTec may process includes:

- Any references obtained during recruitment
- Details of terms of employment
- Payroll details
- Tax and National Insurance information
- Details of job duties
- Details of health and sickness absence records
- Information about performance
- Details of any disciplinary investigations and proceedings
- Training records
- Emergency contact details
- Correspondence with the Company, and other information that you have given to the Company

AccessTec understands that these records are consistent with the employment relationship between the Company and the employee. The data we hold will be used for management and administrative purposes only, but the Company may need to disclose some data it holds about you to relevant third parties. For example, where legally obliged to do so by HM Revenue & Customs, where requested to do so by an employee for the purpose of giving a

reference, or where requested by a client to provide proof of relevant training, qualifications, or experience before carrying out any work.

Sensitive Data

In some cases we may hold sensitive data (as defined in the legislation) about an employee. For example, this could be information about health, racial or ethnic origin, criminal convictions, trade union membership, or religious beliefs. This information may be processed not only to meet the Company's legal responsibilities but, for example, for purposes of personnel management and administration, suitability for employment, and to comply with equal opportunity legislation. Since the processing of this type of information could possibly cause concern or distress, the employee will be asked to give express consent, unless the Company has a specific legal requirement to process such data.

Accessing Data About an Employee

An employee may inspect and/or have a copy of information in your own personnel file and/or other specified personal data and require corrections or deletions should such records be faulty.

Data Security

AccessTec will use appropriate technical and organizational 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 only people who are authorized to use the information can access it. Where possible personal data is to be encrypted.

The employee is responsible for ensuring that any personal data that they hold or process as part of their job role is stored securely. They should ensure that they are aware of any specific requirements to process and secure data in relation to their job role and function within the Company.

The employee must ensure that personal data is not disclosed either orally or in writing, or via web pages, or by any other means, accidentally or otherwise, to any unauthorised third party.

The employee should note that unauthorised disclosure may result in action under the disciplinary procedure, which may include dismissal for gross misconduct. Personal data should be kept in a locked filing cabinet, drawer, or safe. Electronic personal data should be coded, encrypted, or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

When travelling with a device containing personal data, the employee must ensure both the device and data is password protected. The device should be kept secure and where possible it should be locked away out of sight i.e. in the boot of a car. You should avoid travelling with hard copies of personal data where there is secure electronic storage available. When it is essential to travel with hard copies of personal data this should be kept securely in a bag and where possible locked away out of sight i.e. in the boot of a car.

Data Breaches

Should an employee become aware that Company data has been compromised or that there has been a “data breach” they should report this to your line manager and / or AccessTec Data Protection Officer without delay.

The employee should ensure that throughout the course of their employment that they follow all rules in relation to data processing as above. Upon leaving AccessTec they must ensure that all and any data in your possession is returned to the Company. The employee must not retain any confidential information or Company data in any format or medium.

Complied by:	Alex Mountain - Director	17/01/2022	
Authorised by:	Peter King - Director	17/01/2022