Data Protection Policy (GDPR)

Techcon Solutions Limited

This document defines the Data Protection Policy of Techcon Solutions Limited and offers guidance on duties and best practice to users. This document contains the following sections:

- Introduction
- Definitions
- Scope of this policy
- Principles of data handling
- Handling sensitive data
- Sending data to third parties
- Addressing data handling in contracts and agreements
- Taking data away
- Handling Subject Access Requests
- Privacy Policy
- Law Enforcement Requests & Disclosures
- Location and Transfer of data
- Training related to Data Protection, Privacy and Handling
- Notification in case of breach or for other reasons
- Automated Decision Making and Profiling
- Sending bulk email and mail merge communications
- Contact Information

Introduction

Techcon Solutions Limited are required to maintain certain personal data about living individuals for the purposes of satisfying operational and legal obligations. Techcon Solutions Limited recognises the importance of the correct and lawful treatment of personal, sensitive or confidential data. It maintains confidence in the organisation and provides for successful operations.

Techcon Solutions Limited handles a substantial amount of data. Much of this data is private and/or personal data, some is sensitive. When handling the company's data, of any kind, you must always act in accordance with this policy.

The types of personal, sensitive, or confidential data that Techcon Solutions Limited may require includes information about:

- Current, past, and prospective employees/suppliers and others with whom it communicates.
- Current, past, and prospective clients.
- Current, past, and prospective jobs/works/projects.
- Any financial information, such as employee payroll, invoices, purchase orders and contract pricing, not made publicly available.

Any personal, sensitive, or confidential data, whether it is held on paper, computer, or other media, will be subject to the appropriate legal safeguards.

Definitions

For the purpose of this policy, the following definitions apply:

Personal data: any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier (including name, email address, IP address, identification number, location data etc.).

Sensitive data: any data related to racial or ethnic origin, political opinions, religious/philosophical beliefs,

trade union membership, genetic data, biometric data, health data, sex life or sexual orientation, bank account details, debit or credit card details and any data related to children and minors under the age of 13.

Other data: any data that is not personal data or sensitive data.

Scope of this policy

This policy applies to all forms of data handling at Techcon Solutions Limited or on its behalf, manual or automated, in paper, electronic or any other form and to all categories of data without limitation.

Principles of data handling

When handling any data at Techcon Solutions Limited, you should always operate within the following principles:

Principle 1: Lawfulness, Fairness and Transparency

All data at Techcon Solutions Limited shall be processed lawfully and fairly. Where personal data, including sensitive data, is handled, this shall also be done in a manner transparent to the identified or identifiable person to which the data refers. There must always exist a legal basis as defined in the General Data Protection Regulation (GDPR) for the collecting, storing and processing of all data. If in doubt, you must consult with the Office Manager.

Principle 2: Purpose, Limitation and Relevance

Data at Techcon Solutions Limited is collected for specified, explicit and legitimate purposes. This data is never processed in a manner that is incompatible with those purposes. This means that when collecting and/or processing data, you should always specify exactly what the data will be used for and limit any handling and processing to only what is necessary to meet the specified purpose. Where the purpose for processing data is no longer valid or there no longer exists a valid legal basis for it, the data must be securely deleted.

Principle 3: Accuracy

You should always take every reasonable step to ensure that data is accurate and kept up to date. Where data is known to be wrong, it should be rectified without delay. If you are unable to correct the data, you should report any inaccuracies with the aim to get it amended.

Principle 4: Personal and sensitive data held

Unless explicitly allowed by the IT Manager, all personal data and all sensitive data must be held and processed on the Techcon Solutions Limited central server or paper copies kept in secure cabinets.

Principle 5: Storage Limitation and Retention

Personal and sensitive data shall be kept for no longer than necessary for the purpose for which the data is collected, stored and processed. Where possible, data that is retained for historic, statistical or other relevant purposes should be anonymised as much as possible.

Principle 6: Security, Integrity and Confidentiality

All data at Techcon Solutions Limited should always be handled in a manner that is secure and that maintains the data's integrity and confidentiality. All necessary precautions must be taken to protect against unauthorised or unlawful processing, against accidental loss, destruction or damage and against theft.

Handling sensitive data

You must not, under any circumstance, collect, store, access or process sensitive data unless you have been authorised to do by the Office Manager.

Sending data to third parties

Sharing data with third parties must only be done where strictly necessary, in a way that is secure, lawful and fair and with the explicit approval of the Office Manager.

Wherever data is transmitted to third parties, this must always be done using an approved method. Unless not possible for good reason, data should be communicated by direct file upload or other appropriate form of electronic transmission.

Removable media (including USB sticks, external hard drives, CD, DVD, etc) other than the Techcon Solutions Limited's approved encrypted USB sticks must not be used for transmitting data to third parties, unless approved by a Director.

Addressing data handling in contracts and agreements

Managers and other staff responsible for contracts/agreements with third party joint- controllers or data processors must ensure that contracts include appropriate provisions to ensure compliance with the law and with this data handling policy. This must include provisions addressing:

- adherence to the principles as set out above;
- mutual notification of breaches;
- ensuring at all times that there is adequate security of all personal data;
- handling of subject access requests in a timely and complete manner and ensuring that requests received by a third party are passed on to Techcon Solutions Limited without delay.

Taking data away

Where you download, copy or otherwise handle data outside of the Techcon Solutions Limited's office, you must take all appropriate measures to ensure this data remains secure and is not shared, exposed or otherwise compromised in any way. Such data should never be left unsupervised and should never be left behind. Where the data or copy is no longer needed for the purpose for which it was obtained, it must be deleted or disposed of in a secure manner.

Handling Subject Access Requests

All individuals who are the subject of personal data held by Techcon Solutions Limited are entitled to:

- Ask what information the Company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed what the Company is doing to comply with its obligations.

Where a person makes a request ("subject access request") in relation to their personal data, exercising their legal right to:

- Access the information we hold on them ("right of access");
- Request we rectify information we hold ("right to rectification");
- Request we delete their information ("right to erasure");
- Suppress or limit processing of personal data ("right to restrict processing");
- Move, copy or transfer their personal data ("right to data portability");
- Object against processing of their data ("right to object");

D Butler

Duane Butler
Company Director

Date Last Reviewed:
January 2023