



Data Protection Policy

Xpede Medical has documented procedures which define the controls for identification, storage, protection, retrieval, retention time and disposal of records, including external documents where applicable.

Documents are available to those who need and are authorized to access them in line with these retention requirements.

1. Introduction

Xpede Medical Ltd is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

This policy details expected behaviours of Xpede Medical Ltd's Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a Xpede Medical Ltd's Customers and Staff (i.e. the Data Subject) and irrespective of the media used to store the information.

Personal Data is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data.

An organisation that handles personal data and makes decisions about its use is known as a Data Controller. Xpede Medical Ltd as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy.

Non-compliance may expose Xpede Medical Ltd to complaints, regulatory action, fines and/or reputational damage.

Xpede Medical Ltd's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all Xpede Medical Ltd Employees and Third Parties to share in this commitment.

Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction. Breaches of computerized data security have prompted the introduction of legislation on a national and European level.



2. Scope

This policy applies to all Xpede Medical Ltd Entities where a Data Subject's personal data is processed:

- in the context of the business activities of the Xpede Medical Ltd Entity
- for the provision or offer of goods or services to individuals by Xpede Medical Ltd
- to actively monitor the behaviour of individuals.

3. Responsibility

Xpede Medical Ltd ensures that personal data:

- Will be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
- Will be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
- Will be adequate, relevant and not excessive in relation to those purpose(s),
- Will be accurate and, where necessary, kept up to date,
- Will not be kept for longer than is necessary,
- Will be processed in accordance with the rights of data subjects under the Act,
- Will be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
- Will not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information

4. Your Rights

If you are a resident of the European Economic Area (EEA), you have certain data protection rights. If you wish to be informed what Personal Information we hold about you and if you want it to be removed from our systems, please contact us.

In certain circumstances, you have the following data protection rights:

- The right to access, update or to delete the information we have on you.
- The right of rectification.
- The right to object.
- The right of restriction.
- The right to data portability
- The right to withdraw consent



- The right to access, update or to delete the information we have on you.

5. Technical organization and security

The information security policy is intended to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Events classed as Security Incidents or Defects include the following:

- Known breach or attempted breach of security
- Inability (actual or potential) to meet the required customer specification or contract
- Receipt of a formal customer notification or complaint with regard to information security
- Internal audit observation which is classed as a Non-Conformance
- External audit observation which is classed as a Non-Conformance
- Non-Conformance arising from the monitoring and analysis of the ISMS
- Any other event that may require formal investigation and the assignment of corrective or preventive action

Any event listed above shall be brought to the attention of the Information Security Manager for investigation and action. The Information Security Manager shall maintain a log of all events brought to his attention and the action taken.

The Information Security Manager shall investigate any incident or defect brought to his attention and determine whether a formal investigation and response is required. If formal investigation is not required a written response shall be provided, normally by email, on completion of the investigation and a copy placed in the ISMS file. If formal investigation is required a Non-Conformance Report shall be raised either by the Information Security Manager or by the person who raised the incident or defect. The report shall indicate the Corrective Action required.

6. Data Use

Personal data is of no value to Xpede Medical Ltd unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft. Xpede Medical Ltd ensures that:

- When working with personal data, employees will ensure **the screens of their computers are always locked** when left unattended.



- Personal data **will not not be shared informally**.
- Personal data will **never be transferred outside of the European Economic Area**.
- Employees **will not not save copies of personal data to their own computers**.

7. Data Accuracy

The law requires Xpede Medical Ltd to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Xpede Medical Ltd should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff will not create any unnecessary additional data sets.
- Staff will **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.
- Xpede Medical Ltd will make it **easy for data subjects to update the Xpede Medical Ltd holds about them**.
- Data will be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

8. Providing Information

Xpede Medical Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights