Data Protection Policy

Contents

1. Introduction**Error! Bookmark not defined.**
2. Legislation x
3. Registration x
4. Data protection officer x
5. Training x
6. Definitions x
7. Data protection principles x
8. Audit x
9. Privacy notices x
10. Data protection impact assessments x
11. Use of data processors x
12. Rights of data subjects x
13. Procedures x
14. Record keeping x

1. Introduction

This policy outlines the approach taken by Eden Podiatry Clinic Limited to ensure not only that we abide by all United Kingdom (UK) data protection legislation now and in the future, but that a feeling of openness and trust is built between all stakeholders with regard to the security of personal data processed by Eden Podiatry Clinic Limited.

For all of its processing Eden Podiatry Clinic Limited will be the data controller as determined by data protection legislation. (Part 2, Chapter 2 of the Data Protection Act 2018 (DPA) and Article 4(7) of the United Kingdom General Data Protection Regulation (UK GDPR).

2. Legislation

Current legislation governing the use of personal data:

- United Kingdom General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA), including the law enforcement requirements (part 3)
- Privacy and Electronic Communications Regulations 2003 (PECR)

3. Registration

Under the Data Protection (Charges and Information) Regulations 2018, individuals and organisations that process personal data need to pay a data protection fee to the Information Commissioner's Office (ICO), unless they are exempt.

It has been determined that Eden Podiatry Clinic Limited must pay this fee annually. Our registration number is ZA501254.

4. Data protection officer/responsible person

The UK GDPR introduces a duty to appoint a data protection officer (DPO) if you are a public authority or body, or if you carry out certain types of processing activities.

Having reviewed its activities, Eden Podiatry Clinic Limited will not formally appoint a data protection officer however, it will have a nominated person, known as the Responsible Person who will:

- support the development and implementation of UK GDPR compliant policies and procedures within the organisation
- ensure that staff understand and abide by relevant UK GDPR requirements
- support the implementation of UK GDPR compliant activities across the organisation
- be the first point of contact within Eden Podiatry Clinic Limited for any UK GDPR queries
- help Eden Podiatry Clinic Limited demonstrate compliance
- assist in monitoring internal compliance
- act as a contact point for data subjects and
- act as the contact for the supervisory authority (ICO)

5. Training

All employees of Eden Podiatry Clinic Limited will be trained in data protection and their responsibilities relating to information security. This training will be updated regularly at no more than two yearly intervals.

The Responsible Person will undertake the training, or if this is not possible organise an alternative that is, in their opinion, fit for purpose.

6. Definitions

For the purposes of data protection legislation:

'personal data' is anything that can identify a living human being.

'data subject' means an individual who is the subject of personal data.

'data controller' means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

'data processor', in relation to personal data means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

'processing' in relation to information or data means anything at all that is done with the personal data – obtaining, recording or holding it or carrying out any operation or set of operations on it.

7. Data protection principles

The principles are the rules of data protection and Eden Podiatry Clinic Limited must comply with them. The Responsible Person will interpret them in accordance with legislative guidance and advise on their practical application.

They are that personal data be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The UK GDPR also specifies that personal data shall not be transferred outside the UK without appropriate safeguards; the UK-GDPR recognises all EEA/EU countries as ‘adequate’ and upholds existing safeguards prior to its introduction and Article 5(2) of the UK GDPR requires that:

“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

8. Audit

The UK GDPR requires that an organisation records how personal data flows within it.

The Responsible Person will undertake a data protection audit to determine this.

This audit will be a working document to be updated by the Responsible Person as appropriate.

It will be used by the Responsible Person to assist in determining any actions that must be taken to comply with data protection regulations or improve on existing practices.

This document will be reviewed at least annually.

9. Privacy notices

The UK GDPR specifies what individuals have a right to be informed about when you collect and use their personal data. Amongst other things you must tell people why you collect their data, who you share it with and how long you keep it for. Providing people with this information is a key element of the principle of transparency and can also help you to build trust with individuals.

Eden Podiatry Clinic Limited will produce a general privacy notice for clients which will be available on its website and in paper form if it is requested. Applicants for employment and employees will also be given privacy notices specific to them.

Wherever and whenever additional personal data is collected, or existing personal data is to be used for a purpose other than those already specified, there will be a privacy notice specific to the purpose for which the form is being used.

All Eden Podiatry Clinic Limited's privacy notices will be reviewed at least annually.

10. Data protection impact assessments

It is the duty of Eden Podiatry Clinic Limited, where it is the data controller, to undertake a data protection impact assessment (DPIA) if it is unclear whether any processing of personal data, on balance is harmful to the rights and freedoms of the data subjects, or before beginning any processing for a new purpose.

The Responsible Person will decide if a DPIA is required for any processing.

If a DPIA indicates that it has not been possible to determine whether the processing is harmful to the rights and freedoms of the data subjects the matter will be referred to the ICO. Any decision made by the ICO regarding such processing will be binding.

11. Use of data processors

Whenever Eden Podiatry Clinic Limited uses a processor there will be a written contract in place.

The contract is important so that both parties understand their responsibilities and liabilities.

Eden Podiatry Clinic Limited is liable for its compliance with the UK GDPR and will only appoint processors who can provide sufficient guarantees that the requirements of the UK GDPR will be met and the rights of data subjects protected.

Processors must only act on the documented instructions of Eden Podiatry Clinic Limited and penalties may be written into the contract in the event of a breach. They will however have some direct responsibilities under the UK GDPR and may be subject to fines or other sanctions if they do not comply.

12. Rights of data subjects

All data subjects, including children have the right to:

- be provided with a transparent and clear privacy notice which explains who you are and how their data will be processed.
- be given a copy of their personal data;
- have inaccurate personal data rectified and incomplete data completed;
- exercise the right to be forgotten and have personal data erased.
- restrict the processing in specified circumstances;
- data portability;

- object to processing carried out under the lawful bases of public task or legitimate interests, and for the purposes of direct marketing.
- not be subject to automated individual decision-making, including profiling which produces legal effects concerning him or her or similarly affects him or her; See
- complain to the ICO or another supervisory authority;
- appeal against a decision of a supervisory authority;
- bring legal proceedings against a controller or processor; and
- claim compensation from a controller or processor for any damage suffered as a result of their non-compliance with the UK GDPR.

13. Procedures

There shall be procedures for all activities related to the processing of personal data by Eden Podiatry Clinic Limited. Currently these are:

- Data Breaches – Information and Reporting Procedure
- Data Protection by Design Procedure
- Data Protection Impact Assessment Procedure
- Data Subjects' Rights Procedure
- Leavers' procedure
- Subject Access Request Procedure

This list is not exhaustive and procedures may be added to at any time.

14. Record keeping

Article 5(2) of the UK GDPR requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

In order to demonstrate compliance, Eden Podiatry Clinic Limited will keep records of all processing of personal data.

This includes but is not limited to:

- Audit document
- Disclosure log
- List of data subjects' rights exercised
- Minutes of all meetings where data protection and information privacy is discussed

It is the responsibility of all employees to ensure that records remain an accurate reflection of how they work with data.