Data Protection policy

Overview

Key details

- Policy prepared by Craig Barson
- Next review date: May 2020

Introduction

In order to operate, Focus Product Development ("the Company") needs to gather, store and use certain forms of information about individuals.

These can include employees, contractors, suppliers and customers.

This policy explains how this data should be collected, stored and used in order to meet the Companies data protection standards and to comply with the General Data Protection Regulations (GDPR).

Why is this policy important?

This policy ensures that the Company

- Protects the rights of our employees, contractors, suppliers and customers
- Complies with data protection law and follows good practice
- Protect the company from the risks of a data breach

Roles and responsibilities

Who and what does this policy apply to?

This applies to *all* handling data on behalf of the Company e.g.:

- Employees
- Contractors / 3rd party suppliers

It applies to all data that the Company holds relating to individuals, including:

- Names
- Email addresses
- Postal addresses
- Phone numbers
- Any other personal information held (e.g. financial)

Roles and responsibilities

The Company is the Data Controller and will determine what data is collected and how it is used. The Data Protection Officer for the Company is the CEO. They, together with the Management Team, are responsible for the secure, fair and transparent collection and use of data by the Company. Any questions relating to the collection or use of data should be directed to the Data Protection Officer.

Everyone who has access to data as part of the Company has a responsibility to ensure that they adhere to this policy.

The Company uses third party Data Processors to process data on its behalf. The Company will ensure all Data Processors are compliant with GDPR.

Data protection principles

a) We fairly and lawfully process personal data in a transparent way

The Company will only collect data where lawful and where it is necessary for the legitimate purposes of the company.

- An employee's name & contact details will be collected when they first join the company.
    - Lawful basis for processing this data: Contract (the collection and use of data is fair and reasonable in relation to the Company completing tasks expected as part of employment).

- The name of contractors will be collected when they take up a position and will be used to contact them regarding company administration related to their role.

  Further information, including personal financial information may also be collected in specific circumstances where lawful and necessary
    - Lawful basis for processing this data: Contract (the collection and use of data is fair and reasonable in relation to the Company completing tasks expected as part of working with the contractors)

- An individual's name and contact details may be collected when they make a sales purchase or supply a raw material.
    - Lawful basis for processing this data: Contract (the collection and use of data is fair and reasonable in relation to the Company completing tasks),

b) We only collect and use personal data for specific, explicit and legitimate purposes and will only use the data for those specified purposes.

When collecting data, the Company will always provide a clear and specific privacy statement explaining to the subject why the data is required and what it will be used for.

c) We ensure any data collected is relevant and not excessive

The Company will not collect or store more data than the minimum information required for its intended purpose.

d) We ensure data is accurate and up-to-date

The Company will ask employees, customers, suppliers and contractors to check and update their data on an annual basis. Any individual will be able to update their data at any point by contacting the Data Protection Officer.

e) We ensure data is not kept longer than necessary

The Company will keep records for no longer than is necessary in order to meet the intended use for which it was gathered (unless there is a legal requirement to keep records).

The storage and intended use of data will be reviewed in line with the Company data retention policy. When the intended use is no longer applicable (e.g. contact details for an employee who has left the group), the data will be deleted within a reasonable period.

f) We keep personal data secure

The Company will ensure that data held by us is kept secure.

- Electronically-held data will be held within a password-protected and secure environment
- Passwords for electronic data files will be re-set each time an individual with data access leaves their role/position
- Access to data will only be given to relevant employees/contractors where it is clearly necessary for the running of the Company. The Data Protection Officer will decide in what situations this is applicable and will keep a master list of who has access to data

Individual Rights

When the Company collects, holds and uses an individual's personal data that individual has the following the rights over that data. The Company will ensure its data processes comply with those rights and will make all reasonable efforts to fulfil requests from an individual in relation to those rights.

Individual's rights

- *Right to be informed:* whenever the Company collects data it will provide a clear and specific privacy statement explaining why it is being collected and how it will be used.

- *Right of access:* individuals can request to see the data the Company holds on them and confirmation of how it is being used. Requests should be made in writing to the Data Protection Officer and will be complied with free of charge and within one

month. Where requests are complex or numerous this may be extended to two months

- *Right to rectification:* individuals can request that their data be updated where it is inaccurate or incomplete. The Company will request that employees, customers, suppliers and contractors check and update their data on an annual basis. Any requests for data to be updated will be processed within one month.

- *Right to object:* individuals can object to their data being used for a particular purpose. Where we receive a request to stop using data we will comply unless we have a lawful reason to use the data for legitimate interests or contractual obligation.

- *Right to erasure:* individuals can request for all data held on them to be deleted. The Company data retention policy will ensure data is not held for longer than is reasonably necessary in relation to the purpose it was originally collected. If a request for deletion is made we will comply with the request unless:

- There is a lawful reason to keep and use the data for legitimate interests or contractual obligation.

- There is a legal requirement to keep the data.

Right to restrict processing: individuals can request that their personal data be 'restricted' – that is, retained and stored but not processed further (e.g. if they have contested the accuracy of any of their data, the Company will restrict the data while it is verified).

Though unlikely to apply to the data processed by the Company, we will also ensure that rights related to portability and automated decision making (including profiling) are complied with where appropriate.

Data retention policy

Overview

Introduction

This policy sets out how the Company will approach data retention and establishes processes to ensure we do not hold data for longer than is necessary.

It forms part of the Companies Data Protection Policy.

Roles and responsibilities

The Company is the Data Controller and will determine what data is collected, retained and how it is used. The Data Protection Officer for the Company is the CEO. They, together with the Management Team are responsible for the secure and fair retention and use of data by the Company. Any questions relating to data retention or use of data should be directed to the Data Protection Officer.

Regular Data Review

A regular review of all data will take place to establish if the Company still has good reason to keep and use the data held at the time of the review.

As a general rule a data review will be held every 2 years and no more than 27 calendar months after the last review. The first review takes place on 1 June 2018

Data to be reviewed

- The Company stores data on digital documents (e.g. spreadsheets) stored on personal devices held by employees.
- Data stored on third party services

Who the review will be conducted by

The review will be conducted by the Data Protection Officer with other management team member to be decided on at the time of the review.

How data will be deleted

- Physical data will be destroyed safely and securely, including shredding.
- All reasonable and practical efforts will be made to remove data stored digitally.
    - Priority will be given to any instances where data is stored in active lists (e.g. where it could be used) and to sensitive data.

- Where deleting the data would mean deleting other data that we have a valid lawful reason to keep (e.g. on old emails) then the data may be retained safely and securely but not used.

Criteria

The following criteria will be used to make a decision about what data to keep and what to delete.

Question	Action	
	Yes	**No**
Is the data stored securely?	No action necessary	Update storage protocol in line with Data Protection policy
Does the original reason for having the data still apply?	Continue to use	Delete or remove data
Is the data being used for its original intention?	Continue to use	Either delete/remove or record lawful basis for use and get consent if necessary
Is there a statutory requirement to keep the data?	Keep the data at least until the statutory minimum no longer applies	Delete or remove the data unless we have reason to keep the data under other criteria.
Is the data accurate?	Continue to use	Ask the subject to confirm/update details
Where appropriate do we have consent to use the data. This consent could be implied by previous use and engagement by the individual	Continue to use	Get consent
Can the data be anonymised	Anonymise data	Continue to use

Statutory Requirements

Data stored by the Company may be retained based on statutory requirements for storing data other than data protection regulations. This might include but is not limited to:

- Invoices
- Delivery Notes
- Meeting minutes
- Contracts and agreements with suppliers/customers
- Insurance details
- Tax and employment records
- Clinical Evaluations

Other data retention procedures

Employee data

- When an employee leaves the Company and all administrative tasks relating to their employment have been completed any potentially sensitive data held on them will be deleted
- All other data will be stored safely and securely and reviewed as part of the next two year review

Other data

- All other data will be included in a regular two year review.