Policy

Data protection

Procedure Reference BMSP-37 Issue 5

26/02/2018

First Full Issue

Table of Contents

1 The purpose of this policy

The purpose of this policy is to detail Fundamentals' commitment to data protection throughout the organisation. This policy is appropriate to the Company's activities and is available to all staff and stakeholders.

It sets objectives and is subject to periodic review and improvement.

1.1 The policy

Fundamentals will comply with all applicable data protection legislation and good practice.

1.1.1 The Company will only process personal information where strictly necessary for operational, legal or regulatory purposes.

1.1.2 Only the minimum amount of personal information required for these purposes will be processed. This personal information will be relevant and adequate. The company will keep the information accurate and up to date.

1.1.3 The Company will provide clear documented details to persons on how their personal information can be used and by whom [link to documents].

1.1.4 Special documented safeguards must be in place if information is gathered directly from children.

1.1.5 The Company will collect and process information fairly and lawfully.

1.1.6 A documented inventory will be maintained of the categories of personal information processed by the company. The purpose of each category will also be documented including explicitly high-risk categories of personal information.

1.1.7 Personal information will be accurate and where necessary up to date.

1.1.8 The Company operates a data retention policy. [*Link]*

1.1.9 The Company respects persons rights in relation to their personal information and will maintain easily accessible records of privacy information provided to individuals and consents received before the collection of the data.

1.1.10 All personal information will be kept secure and only transferred outside the UK where it can be adequately protected. Any data sharing will be covered by a written agreement or contract between

both parties documenting the responsibilities of both parties. Individuals have the right to data portability and data will be transferred to them or their nominees free of charge.

1.1.11 Employees with specific roles, responsibility and accountability for data protection will be identified.

1.1.12 Interested parties are identified in the interested party document ..\..\Business System\BMSP-10 Company and context.pptx

1.1.13 The Company has a procedure for addressing data protection breaches see 7.0

2 Employees

2.1 Your rights as an employee

2.1.1 All employees will be made aware of the nature of information stored about them, its source, how it will be used and who it will be disclosed to.

2.1.2 Employee consent may be required to collect some sensitive data.

2.2 How to access your data – a Subject Access Request

2.2.1 Employees have a right to gain access to information about them held by the company, by means of an access request.

2.2.2 The company will process the requests and respond promptly in any case within 1 month, this may be extended in the case of complex requests.

2.3 Your Privacy Notice

2.3.1 The company will only collect and process the personal information about employees that it requires to run its business within the law. All information will be handled properly and stored and processed securely. The privacy notice will contain the lawful basis and the intended purposes of processing the data. The privacy notice can be found here Privacy Notice - Employees.docx

3 Customers and Contacts

3.1 Your rights as a customer or contact

3.1.1 All customers and contacts will be made aware of the nature of

information stored about them, its source, how it will be used and who it will be disclosed to.

3.1.2 Consent may be required to collect some sensitive data.

3.1.3 Consent requests will be prominent, concise, easy to understand and separate from any other information such as general terms and conditions. Consent may be withdrawn at any time.

3.2 How to access your data – a Subject Access Request

3.2.1 Customers and contacts have a right to gain access to information about them held by the company, by means of an access request.

3.2.2 The company will process the requests and respond promptly in any case within 1 month, this may be extended in the case of complex requests.

3.3 Your Privacy Notice

3.3.1 The company will only collect and process the personal information about customers and contacts that it requires to run its business within the law. All information will be handled properly and stored and processed securely. The privacy notice will contain the lawful basis and the intended purposes of processing the data.

4 Suppliers, Consultants and Sub-contractors

4.1 Your rights as a supplier, consultant or sub-contractor

4.1.1 All suppliers, consultants and sub-contractors will be made aware of the nature of information stored about them, its source, how it will be used and who it will be disclosed to.

4.1.2 Consent may be required to collect some sensitive data

4.1.3 Consent requests will be prominent, concise, easy to understand and separate from any other information such as general terms and conditions. Consent may be withdrawn at any time

4.2 How to access your data – a Subject Access Request

4.2.1 Suppliers, consultants and sub-contractors have a right to gain access to information about them held by the company, by means of an access request.

4.2.2 The company will process the requests and respond promptly in any case within 1 month, this may be extended in the case of complex requests.

4.3 Your Privacy Notice

4.3.1 The company will only collect and process the personal information about suppliers, consultants and sub-contractors that it requires to run its business within the law. All information will be handled properly and stored and processed securely. The privacy notice can be found here Privacy Notice - Exterrnal.docx.

4.4 Processing of information by contractors or suppliers.

4.4.1 The company will ensure where personal data is processed on its behalf by a contractor, the contractor will be pre-audited to ensure they can provide the required level of security. Once selected a contract will be put in place governing the relationship.

5 Rectification, Erasure and Restriction

5.1 Rectification

5.1.1 Once made aware of an error the company will without undue delay rectify any incorrect or incomplete information about a natural person.

5.2 Erasure

5.2.1 The company will ensure that right to erasure requests from natural persons are promptly and appropriately handled without undue delay.

5.2.2 The company will erase the data if it falls within the categories defined within the act.

5.2.3 Where the information has been made public the company will take measures to inform other companies who may be processing the information that an erasure request has been made.

5.3 Restriction

5.3.1 The company will ensure individuals have the right to restrict information processing when applicable.

5.3.2 The requester will be informed if a restriction is going to be lifted.

6 Objections, Complaints and Appeals

6.1 Objections

6.1.1 The company will consider and respond to requests from individuals who object to information processing.

6.1.2 If the request is an objection to processing for direct marketing purposes the company will ensure processing ceases.

6.2 Complaints and appeals

6.2.1 The company will ensure complaints about the processing of personal information are handled correctly, this will include appeals to the objections procedure.

6.3 Manifestly unfounded or excessive requests

6.3.1 Manifestly unfounded or excessive requests can be charged for or refused. When making a subject access request you should consider carefully what information you require and why to ensure that your request can be dealt with quickly and effectively. Submit your request to us setting out the grounds for your request. Your request will be acknowledged and you will be advised when you can expect to receive the information you requested and any other information relevant to processing your request.

7 Data Breaches

7.1 Detecting and investigating data breaches

7.1.1 The company will monitor for data breaches and in the event of detecting a breach investigate the cause of the breach and its potential impact on individuals.

7.2 Notification of data breaches

7.2.1 In the event that a breach is likely to result in a risk to the rights and freedoms of individuals, the ICO will be notified within 72 hours by the Finance Director.

7.2.2 In the event that a breach is likely to result in a high risk to the rights and freedoms of individuals, they will be notified individually without undue delay by the Finance Director.

8 Training and Awareness

8.1 Training and awareness

8.1.1 The company will ensure that all employees and contractors are aware of their responsibilities when processing personal information.

8.1.2 The company will ensure the training and awareness maintains and improves information protection requirements and practice.

9 Appendix (extracts from the Regulations)

9.1 The six categories of lawful processing

Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks

9.2 Consent guidelines

The GDPR sets a high standard for consent.

• Doing consent well should put individuals in control, build customer trust and engagement, and enhance your reputation.

• Check your consent practices and your existing consents. Refresh consents if they don't meet the GDPR standard.

• Consent means offering individuals genuine choice and control.

• Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of consent by default.

• Explicit consent requires a very clear and specific statement of consent.

• Keep your consent requests separate from other terms and conditions.

• Be specific and granular. Vague or blanket consent is not enough.

• Be clear and concise.

• Name any third parties who will rely on the consent.

• Make it easy for people to withdraw consent and tell them how.

• Keep evidence of consent – who, when, how, and what you told people.

• Keep consent under review, and refresh it if anything changes.

• Avoid making consent a precondition of a service.

• Public authorities and employers will find using consent difficult.

• Remember – you don't always need consent. If consent is too difficult, look at whether another lawful basis is more appropriate.

9.3 Approved By (Signature):

Jon Hiscock

Managing Director

Date: 13.03.2018