Data Protection Policy

for

Beeswift Ltd.

Policy effective from 11/06/2018

Last Updated by Beeswift Ltd.

Version History

Change Date	Author	Change	Next Review Date
11/06/2018	Ebit Consultancy Ltd.	Initial Version	11/06/2019
11/06/2019	Beeswift Ltd.	Review	11/06/2020
11/06/2020	Beeswift Ltd.	Review	11/06/2021
11/06/2021	Beeswift Ltd.	Review	11/06/2022

Contents

1 Purpose

1.1 Introduction

Under the General Data Protection Regulation and Privacy and Electronic Communications Regulation (2003), Beeswift Ltd. needs to gather and use certain information about individuals, and ensure it does so in a legal, fair and responsible manner.

These individuals can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards, and to comply with the law.

1.2 Why this policy exists

This Data Protection policy ensures Beeswift Ltd.:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

1.3 Intended Audience

The document is intended to be read by all members of Beeswift Ltd. who have dealings with personal data.

1.4 Data Protection Law

The European Union General Data Protection Regulation (GDPR) 2018 (to be enforced in the UK as part of the Data Protection Bill 2018) describes how organisations – including Beeswift Ltd. – must collect, handle and store personal information.

GDPR supersedes all national regulations including the U.K. Data Protection Act 1998 providing a revised set of rules and principles. As this is more strictly defined and enforced than existing national rules, this policy is in compliance with GDPR.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The General Data Protection Regulation is underpinned by six important principles. These say personal data must:

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

2) 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;

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

4) 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;

5) 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 GDPR in order to safeguard the rights and freedoms of individuals;

6) (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.

As a Data Controller, Beeswift Ltd. is responsible for and be able to demonstrate compliance with the principles.

2 People, Risks and Responsibilities

2.1 Policy Scope

This policy applies to:

- The head office of Beeswift Ltd.
- All staff and volunteers of Beeswift Ltd. wherever they are working
- All contractors, suppliers and other people working on behalf of Beeswift Ltd.

It applies to all data that the company holds relating to identifiable individuals, even if that information technical falls outside the GDPR 2018. This can include:

- Names of individuals
- Postal Addresses
- email addresses
- telephone numbers
- any other information which can be directly used to identify an individual

2.2 Data Protection Risks

This policy helps to protect Beeswift Ltd. from some very real compliance risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

2.3 Responsibilities

Everyone who works for, or with Beeswift Ltd. has some responsibility for ensuring data is collected, stored and used appropriately.

Everyone that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

Within the business, the following roles have key areas of responsibility:

- the board of directors is ultimately responsible for ensuring that Beeswift Ltd. meets its legal obligations.
- David Griffin, Financial Director, is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- reviewing all data protection procedures and related policies, in line with an agreed schedule.
- arranging data protection training and advice for the people covered by this policy.
- Dealing with requests from individuals to see the data Beeswift Ltd. holds about them (also called 'subject access requests').
- checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from schools, parents, journalists or media outlets.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.
- Ensuring all marketing lists have appropriate consent for all individuals on the list prior to using them, and ensuring the introductory contact follows the correct procedures.

- faIT UK Ltd. (The IT Provider), is responsible for:
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

3 General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Beeswift Ltd. will provide training to all employees to help them understand their responsibilities when handling data.

- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
    - In particular, strong passwords must be used and the should never be shared.
    - If sending any personal information outside the organisation, always password protect it then call the recipient and tell them the password.
    - Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

4 Collection of personal data

In general, Beeswift Ltd. only requires personal information for marketing or contractual purposes. It will not hold any form of personal information on behalf of customers or suppliers.

Beeswift Ltd. only collects the following personal data:

What is collected?	**How is it processed?**
Email address, name	Direct marketing Held on email system and email distribution system
Names, addresses, employment and payroll information, certificates of qualifications. Health certification (where required) Right to work documentation	HR Information. This is the standard HR contractual and legally required information to operate a contract of employment.
Names	HSE Incident Reporting This is a legal requirement.

4.1 Collection of sensitive personal data

Sensitive Personal Data includes information such as:

- Racial or ethnic origin;
- Political belief or opinion;
- Religious or similar beliefs;
- Sexual orientation;
- Trade Union Membership;
- Physical or mental health condition;
- Criminal offences or alleged offences committed;

Beeswift Ltd. has no justification or requirement to collect or process any such information and will refuse to do so.

If any such data is received in error, it will be destroyed immediately.

5 Data Classification

By being able to classify information based on its sensitivity, it becomes easier to manage the risks associated with that piece of information.

In general, all personal information is classified as high risk.

5.1 Terminology

Classification	Definition	Impact of loss
Personal data	any item of data which can uniquely, or when combined with other data can identify an individual.	High
Sensitive personal data	any data about an individual (such as sexuality, or religious or political beliefs) which could prejudice the rights and freedoms of an individual if it became known about them.	High

Classification	Definition	Impact of loss
Company data	any data about a company (whether customer, supplier or sub-contractor) which does not include any form of personal data. This includes publicly available contact information, locations and so on, as well as confidentiality agreements and any terms of reference	Low
Confidential data	data about an individual or company which has extremely restrictive access. Such information includes contractual data and accounts.	High
Company confidential data	data which must not leave the business such as policies and procedures, passwords to access shared data.	High
Client data	any client information which is held or retained in order to fulfil a current or previous contractual obligation.	Moderate
Public data	Information which is in the public interest and becomes publicly available following publication	Low

5.2 Classifying data

All data is to be classified according to one of the terms above. Unless a tagging mechanism is available, it is suggested that the filename should include the chosen classification. Only one classification applies to a file at any one time.

5.3 Protection

Impact of loss	Protective Measures
High	Ensure all data is encrypted where technically possible and only accessible to people who need access to it
Moderate	Ensure data is held in encrypted directories with restrictive access
Low	Data can be held unencrypted

5.4 Recommended Classifications

Type of information	Data Classification
Direct Marketing	Personal Data
HR Information	Sensitive Personal Data
HSE Incident Reporting	Confidential Data.

6 Data Retention

Data is only to be held for the minimum time it is required.

The business should examine each type of information it processes after each review period to identify which pieces of information are now obsolete and therefore due for secure deletion or destruction.

In most cases, this can be automated, so no effort will be required on behalf of the business to perform this housekeeping.

It is suggested that where further consent is required from the customers, this is requested after the review period has elapsed and that customers are given a further month to respond before their information is removed from the system.

Type of information	Retention Period	Review Period	Commentary
Direct Marketing	12 months	6 months	Check back with the customer if they are interested in further advertising. If the customer is not interested, they must be removed from the list
General HR information	7 years	6 months	This information can safely be deleted 7 years after the employee finished employment.
HSE Incident Reporting	Indefinite		This is to fulfil the legal requirements
Sales Orders	2 years maximum	Annual	This can be amended to a longer period where required for guarantee/warranty purposes
Invoices	7 years	6 months	This is determined by HMRC guidelines

Type of information	Retention Period	Review Period	Commentary
Payroll data for accounting	2 months	Monthly	This is only the working information which is transferred from The National Access & Scaffolding Confederation to the accountants and as such is transient.

7 Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to faIT UK Ltd.

When data is stored on paper, it should be stored in a secure location where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- All data is to be recorded in the Data Asset Register, classified and named according to the Data Classification rules and retained only for as long as defined in the Data Retention rules.
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a removable disk, DVD or USB memory storage), these should be kept locked away securely when not being used.
- All storage devices used to hold data must be fully encrypted at device level by default.
- Data classified as personal or confidential is to be encrypted irrespective of its storage location.

- Data is only to be stored on designated drives and servers and must only be uploaded to Beeswift Ltd.'s approved cloud computing services.
- Servers containing data will be sited in a secure location, away from the general office space.
- Data should be backed up frequently. These backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones except where doing so is to a designated directory as part of a cloud-hosted file sharing mechanism.
- Data may not be accessed using approved personal devices (which are not owned by Beeswift Ltd.)
- All servers and computers containing data should be protected by approved security software and a firewall

7.1 Data purging

Data purges should take place on a monthly basis determined by the retention period and reviews of the Data Asset Register.

7.2 Personal Data Storage

Personal data is only to be stored on the following providers:

- Microsoft Exchange for email archiving and personal contact lists
- On-site file servers for all business file storage
- DropBox for cloud file sharing -This is only to be used for external customers where we are supplying Media and documents that are already in the public domain
- SAGE for Payroll
- SendInBlue for bulk e-mail campaigns and internal distribution of staff newsletters
- Varnet the company ERP system

All other providers and locations should not be used for storing personal data.

8 Data Use

Personal data is of no value to Beeswift 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:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Beeswift Ltd. must only hold the minimum amount of personal information required for contractual or marketing purposes. Any other personal information received from or about the individual must be destroyed.
- The individual must give their explicit consent for Beeswift Ltd. to hold and process their data. They must be clearly and unambiguously informed as to the type of information required, its purpose, how and where it will be held and their rights of access and alteration.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Sensitive personal data is not required at all by Beeswift Ltd. and is to be destroyed immediately if it is accidentally received.
- All identity related documentation from individuals is only required to verify their identity. It should be handled as follows:
    - It should be logged in the Data Asset Register
    - It must be encrypted when it arrives (unless it is received in an encrypted format);
    - It must only be unencrypted at the time it is to be reviewed.
    - All versions of it must be destroyed as soon as it's intended purpose is complete and this must be logged in the Data Asset Register.
- Data must be encrypted before being transferred electronically.
    - Files containing the data are to be encrypted using a complex password generated by, and subsequently stored in the shared password manager storage area. The encrypted files are to remain in the same location as the original data.
    - The filenames and a description of their contents are to be logged in the Data Asset Register with the employee's name, the date of the transfer, the destination for the encrypted data and reason for the transfer.
    - The encrypted files can then be transferred using the required method.
    - When the destination receives the files, the password is then to be sent using a separate and different method to the data transfer. In general, it is recommended that a text message is used. Verify the recipients phone number first then send a message which contains the password and nothing else.

- Personal data must never be transferred outside the European Economic Area or to a country designated by the EU as a 'Second Country' (which includes the UK). If in doubt, ask the Data Protection Officer first.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.
- All data relating to individuals must be factual. No opinionated or subjective data is to be held anywhere on Beeswift Ltd.'s systems.

9 Data Accuracy

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

The more important it is that personal data is accurate, the greater the effort Beeswift 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 accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Beeswift Ltd. will make it easy for data subjects to update the information it holds about them. For instance, via email.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, they should be contacted by an alternative method and if that doesn't get a response, then it should be removed from the database.
- It is the Marketing Manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.
- Individuals can formally request amendments to their data via an email. Instructions for this are listed on the website.

10 Subject Access Requests

All individuals who are the subject of personal data held by Beeswift Ltd. 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 how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a 'subject access request'.

Subject access requests from individuals should be made by email addressed to the data controller at dataofficer@beeswift.com. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals cannot be charged for subject access requests. The data controller will aim to provide the relevant data within 1 calendar month of the request being verified.

If they are unable to do so, they must notify the individual within 1 calendar month of the request being received as the reason for failing to do so.

The data controller must always verify the identity of anyone making a subject access request before handing over any information. Any personal information provided by the individual to do so must be logged in the Data Asset Register and destroyed as soon as the identity is verified.

11 Data Portability

All individuals who are the subject of personal data held by Beeswift Ltd. are entitled to request copies of their data to be provided in a common format suitable for transfer to a designated third-party.

This can be requested through the 'Subject Access Request' process. All data is to be provided in a CSV tabular format. The resultant file is then to be encrypted and transferred according to the process described in 'Data Use'.

The original text file is to be destroyed immediately. The encrypted file can be destroyed once the recipient has successfully received and verified the contents of the file.

12 Handling Data Breaches

Beeswift Ltd. takes the protection of data very seriously but there will be occasions when something goes wrong, and data is 'lost'.

As long as the appropriate procedures have been followed, the impact on individuals, customers, suppliers and staff will be minimal. This is one of the reasons for this policy and ensuring all employees adhere to it.

12.1 When to report them

If the data which is lost is suitably encrypted and the password has not been sent or compromised by the recipient, there is no need to notify the Information Commissioners Office.

If data about individuals has been 'lost' which is not encrypted, this presents a serious risk to the individuals rights and to Beeswift Ltd.

Under this circumstance, the Data Protection Officer must notify the Information Commissioners Office within 72-hours of becoming aware of the breach.

Where the breach is likely to significantly affect the rights of individuals, the individuals must also be notified of the breach.

12.2 What needs to be in the breach notification?

- The nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned;
- The name and contact details of the data protection officer where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

12.3 Identifying the cause of the breach

This is not to be a 'witch-hunt' to find someone to point the finger of blame at. Everyone is human and occasionally prone to mistakes.

This is why there is a process for handling Data Storage and Data Use and as long as both are being followed, it should be straightforward to determine the cause of the breach.

Where the breach is as a result of an externally originated compromise, the supplier must notify Beeswift Ltd. accordingly.

12.4 Learning from the breach

A breach can easily be as a result of a failed procedure or an unexpected gap in an existing procedure and it is important that this is understood, documented and used to provide constructive feedback into refining the affected procedure.

Where the breach is as a result of deliberate non-compliance with the procedures, this is far more serious and will be met with disciplinary measures. Under this circumstance, the Data Protection Policy must then be reviewed with further staff training being a possible outcome.

13 Providing Information

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

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

To this end, the company has a privacy statement, setting out how data relating to individuals is used by the company.

This is available on request. A version of this statement is also available on the company's website.