Marketing 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	EbitConsultancy 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 ensure it carries out all marketing and electronic customer communications in a legal, fair and responsible manner.

This means individuals receiving electronic marketing messages (and other forms of non-contractual communication) must have the ability to easily give and revoke permission to receive these messages.

This does not include any communication between Beeswift Ltd. and the individual which is required for the negotiation or fulfilment of a contractual obligation by either party.

This policy describes what is permitted and any processes required in order to comply with the law.

1.2 Why this policy exists

This marketing policy ensures Beeswift Ltd.:

- Complies with data protection law and follows good practice
- Protects the rights of its customers and partners
- Performs marketing activities in a legal, consistent and respectful manner

1.3 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. It also specifies the rights of individuals in determining how, and for what purposes their data may be used by organisations in furthering their legitimate business interests, especially regarding marketing.

Further to this, the Privacy and Electronic Communications Regulation (2003) (PECR) details the methods and protocols by which marketing messages may be provided to individuals. This must be considered alongside the GDPR to provide the overall set of rules governing all marketing and electronic communications.

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 be:

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.

Also, all individuals have 8 rights which must be upheld by organisations using their information. Of these the following are relevant in the context of marketing:

1) The right to be informed – all organisations must let individuals know precisely how their personal information will be used;

4) The right to erasure – where an organisation is using an individual's information in an inappropriate way or the individual decides they no longer wish that organisation to use their information for a non-contractual

purpose, the organisation must delete that individual's information at their request.

7) The right to object – if an individual's personal information is being used for purposes which they have not agreed to, the individual has the legally enforceable right to prevent the organisation from using that information. This can be in circumstances where there is no other legal basis for the organisation to process that information, or where the individual has not given permission for the organisation to use their information in the way it is being used.

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 newsletters and marketing messages sent out electronically by Beeswift Ltd. as part of its normal operations.

2.2 Marketing Compliance Risks

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

- Marketing with individuals without their permission.
- Using an individual's personal data for marketing purposes when they have never consented to allowing it to be used for such.
- Reputational damage. For instance, the company could suffer if they were caught in violation of the GDPR and/or PECR and were named and shamed on the ICO Offenders page.

2.3 Responsibilities

Everyone who works for, or with Beeswift Ltd. has some responsibility for ensuring data is collected, stored and used appropriately. Beeswift Ltd. has responsibility to ensure appropriate measures are in place to ensure it is used solely for the purposes for which it was collected and prevent its misuse.

Everyone responsible for communicating with individuals using electronic means will be responsible for ensuring they adhere to this policy.

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, acting as The Data Protection Officer for Beeswift Ltd. is responsible for:
    - ensuring the Editorial and Sales and Marketing teams are familiar with this policy and operate in an appropriate manner to maintain a balance between the legitimate interests of the company and fulfilling the rights of the individuals.
- James Fellows, is responsible for:
    - Ensuring all newsletter communications are only sent to people who have requested them;
    - Ensuring telemarketing plans and operations are performed according to the principles and processes detailed within this policy;
    - Ensuring the technical mechanisms for linking consent and individual's permissions and choices are synchronised to prevent a situation where an individual removes their consent on one system only to receive marketing from another.

3 Marketing Principles

Beeswift Ltd. has a responsibility to ensure all marketing and electronic communications are carried out firstly, in line with ensuring it protects the rights of individuals, and secondly balancing up the legitimate interests of the business.

Information Security has three basic principles detailed as follows:

3.1 Individual Rights First

At all times, the individual has the right to decline to receive direct marketing. Violation of this right is punishable under the GDPR to the maximum legally enforceable amount so doing so would have a significantly adverse effect on the business and should be avoided.

Individuals should be given multiple, explicit choices regarding marketing and what they wish to receive.

3.2 Legitimate Interests of the Business

Under clarification of the GDPR determined by the ICO and the Direct Marketing Association, businesses which provide direct marketing services (such as Beeswift Ltd.) have legitimate business interests in providing marketing services to individuals.

Where no other legal basis exists for the business to communicate with the individual, the business can perform a Legitimate Interest Assessment.

This effectively comprises of the following 3 tests:

1) Purpose Test: Is the purpose a legitimate business interest
2) Necessity Test: is the processing of individual information necessary for that purpose?
3) Balancing test: do the individual's rights override the legitimate interest?

In the case of this business,

- the purpose test will be answered by the commercial interests of the business;
- the necessity test means that the information used must be targeted and proportionate which signing up to the newsletter, or relying on the 'soft opt-in' mechanism (see section 5.1 - Existing or Previous Customers) would certainly be;
- finally in terms of balancing the commercial interests of the business against the individuals interests, the business must consider if contacting the individual would be likely to cause distress or harm to that individual.

If all 3 elements of this test are positive, this must be recorded (in a spreadsheet would be adequate) prior to starting the advertising campaign.

This would generally imply that the newsletters would be in the legitimate interests of the business and can therefore be sent without issue so long as the individual has not already chosen not to receive them.

3.3 Consent must be freely given

Individuals cannot be coerced into providing consent for marketing purposes. nor can consent be obtained as a condition of the business providing them a service.

See section 6 - Giving the individual control

3.4 Consent must be explicit

Where consent is the only valid legal basis for marketing to the individual, the marketing messages must only be in relation to choices the individual has already made.

For instance, if an individual has given their consent to receive special offers regarding advertising, the same permission does not apply to receiving messages about new products.

See section 6 - Giving the individual control

3.5 List Management

If an individual chooses to be removed from a marketing list, they must be removed from that list irrespective of any commercial interest in retaining them.

It is recommended that existing marketing lists are either deleted if the individuals within them have not been contacted for a period of 18 months or more.

3.6 Communication Frequency

If an individual chooses to receive marketing communications, the business must check periodically with the individual to verify their ongoing permission to do so.

This frequency will be defined in the Data Retention and Housekeeping Policy.

The user must be given a choice as to whether they wish to carry on receiving marketing messages.

A non-reply cannot be taken as acceptance so any individual who does not respond must be removed from the marketing lists.

4 Newsletters

Under the current legislation, newsletters can be determined to be marketing messages unless they contain no advertising (which is unlikely in this context).

Therefore, the newsletter processing must follow the same rules as other marketing and ensure the individuals have a means of adding or removing their consent easily.

Most mailshot systems include the option to add an ‘unsubscribe’ option to the end of the newsletter which will be adequate for the purposes of GDPR compliance.

The same facility can also be used to allow the individual to amend their details thus ensuring the accuracy of the information and again allowing compliance with GDPR.

5 Marketing Communications

5.1 Existing or Previous Customers

For customers where there has been an existing business relationship, this provides the business with the so-called 'soft opt-in' option which means it can continue to market related products or services only without requiring the explicit consent of the individual.

It must be noted though that this only applies to the subsequent marketing of the same products or services which the individual has already purchased, and it must be done in a relevant and timely manner after the original transaction.

This means the business must get separate consent from the individual if it wishes to market a different product or service.

5.2 New Customers

Where a new customer initiates the conversation with the business, they will need to give their explicit consent to be marketed to.

This should either be using a website registration process or by means of recording the time and date on which consent was given if the conversation was via the telephone system.

Whichever method is used, there must be a record that the individual explicitly gave their consent.

5.3 Marketing Lists and Prospects

When communicating with an individual from a marketing list, or someone identified as a suitable prospect for the first time, the business must follow the standard PECR process and gain the individuals consent before providing them with the marketing message.

Failure to do so will be taken as a violation of both PECR rules, the GDPR principles of transparency, purpose limitation and the rights regarding consent.

It is suggested that any individuals who are 'prospected' should have their identities and contact details verified using a search engine prior to contacting them.

5.4 Telemarketing

When opening up a conversation with a prospect, it is suggested that the call logging systems is enabled prior to asking and requesting permission to carry on the conversation.

This will be necessary to prove the individual gave their consent if required.

The correct process will therefore follow this flow:

1) Introduce yourself as from Beeswift Ltd. and explain a little about what they do;
2) Explain where the contact information was obtained from;
3) Enable the call recording facility;
4) Ask for permission to talk to the individual regarding marketing conversation.
5) If they say No, politely end the call and remove them from the marketing list;
6) If they say yes, record the fact they have given their consent in the CRM and stop recording the call unless required to do so for other reasons;
7) Carry on the conversation as required
8)

6 Giving the individual control

GDPR requires businesses provide simple methods of giving or removing consent and maintaining the accuracy of an individual's personal information.

At present though all systems are disconnected from each other meaning that if an individual changed their permissions in one area the changes are not reflected across all systems. This is particularly obvious with the disconnect between registration for the newsletter and advertising systems.

To avoid unintended consequences of this, it is recommended these all feed into a single system such as those used for mailshots even if the business does not require such a system for that purpose.

6.1 Electronic Mail Permissions

It is recommended that mailing tools such as MailChimp or SendInBlue are used to manage all electronic mail communication as these provide simple mechanisms by which individuals can manage their own preferences and consent. This puts control of the process back into the hands of the individual rather than the company.

These can typically easily integrate with most CRM systems.

6.2 Website Permissions

The existing website login and registration systems provide mechanisms by which an individual can maintain their preferences, but they must do so in multiple places.

This information should be fed in to the CRM and ideally into to the mailshot systems where individuals can then manage their preferences.

6.3 Telephone Preference Service/Mail Preference Service

Irrespective of the method to use all contact information to be used in mailshots or marketing campaigns should be processed against the details held in the Telephone Preference Service and Mail Preference Service lists prior to distribution.