Data Protection Policy

Introduction

Bostonair Group (and all Associated Companies) needs to gather and use certain information about individuals and companies in order to fulfil its service requirements. These individuals 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 General Data Protection Regulations 2018 (GDPR).

Policy scope

This policy applies to all staff, who must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

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

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus, any other information relating to individuals

Terms and definitions

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes include the following: • Compliance with our legal, regulatory and corporate governance obligations and good practice • Ensuring business policies are adhered to • Operational reasons, such as recording transactions, training and

	quality control, ensuring the confidentiality of commercially sensitive information and pre-employment vetting • Investigating complaints • Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments • Monitoring staff conduct, disciplinary matters • Marketing our business • Improving services
Personal data	'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.
Data controller	'Data controller' means the legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.
Data processor	'Processor' means a legal person, which processes personal data on behalf of the controller.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office (ico).

Responsibility for the policy

As our data protection officer (DPO), Michelle Bisby has overall responsibility for the day-to-day implementation of this policy. You should contact the DPO for further information about this policy if necessary.

Bostonair Group shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles.

The Principles are:

1. Lawful, fair and transparent

   Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.
2. Limited for its purpose

   Data can only be collected for a specific purpose.
3. Data minimisation

   Any data collected must be necessary and not excessive for its purpose.
4. Accurate

   The data we hold must be accurate and kept up to date.
5. Retention

   We cannot store data longer than necessary.
6. Integrity and confidentiality

   The data we hold must be kept safe and secure.

Accountability and transparency

We must ensure accountability and transparency in all our use of personal data. We must show how we comply with each Principle. You are responsible for keeping a written record of how all the data processing activities you are responsible for comply with each of the Principles. This must be kept up to date and must be approved by the DPO.

To comply with data protection laws and the accountability and transparency Principle of GDPR, we must demonstrate compliance. You are responsible for understanding your particular responsibilities to ensure we meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments
- Implement measures to ensure privacy by design and default

Why this policy exists

This data protection policy ensures Bostonair Group:

- 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

Data protection law

The General Data Protection Regulation 2018 (GDPR) describes how organisations including Bostonair Group, must collect, handle and store personal information.

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

In line with GDPR, Bostonair Group has established that it's lawful basis for processing data is Contract, Article 6(1)(b) where:

'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'

Data protection risks

This policy helps to protect Bostonair Group from some very real data security 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.

Responsibilities

Everyone who works for or with Bostonair Group has some responsibility for ensuring data is collected, stored and handled appropriately.

Company's responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful

- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised

Employee's responsibilities

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

These people have key areas of responsibility:

The board of directors is ultimately responsible for ensuring that Bostonair Group meets its legal obligations.

- The data protection officer, Michelle Bisby, is responsible for:
  - Keeping the board updated about data protection responsibilities, risks and issues
  - Reviewing all data protection procedures and related policies on a regular basis
  - Arranging data protection training and advice for the people covered by this policy
  - Handling data protection questions from staff and anyone else covered by this policy
  - Responding to individuals such as clients and employees who wish to know which data is being held on them by us
  - Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

The IT coordinator, Aidan Gardner, 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.

The marketing manager, Tom Anderton, is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

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.
- **Bostonair Group 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 they should never be shared.
- 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.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

Data storage and security

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is **stored on paper**, it should be kept in a secure place 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:

- 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 CD or memory stick), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services.**
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those 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.
- All servers and computers containing data should be protected by **approved security software and a firewall.**

Data Use

Personal data is of no value to Bostonair Group 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.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.
- Employees **should not save copies of personal data to their own computers**. Always access and update the central copy of any data.

Data Accuracy

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

The more important it is that the personal data is accurate, the greater the effort Bostonair Group 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 as 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.
- Bostonair Group will make it **easy for data subjects to update the information** Bostonair Group holds about them. For instance, via the company website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, 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.

Rights of individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. Right to be informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

- Enabling individuals to access their personal data and supplementary information
- Allowing individuals to be aware of and verify the lawfulness of the processing activities

3. Right to rectification

- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay, and no later than one month. This can be extended to two months with permission from the DPO.

4. Right to erasure

- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

- We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

- We must respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

Disclosing Data for Other Reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Bostonair Group will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Privacy notices

A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which mean within one month.

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

Privacy notices must be concise, transparent, intelligible and easily accessible.

The following information must be included in a privacy notice to all data subjects:

- Identification and contact information of the data controller and the data protection officer
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the ICO, and internal complaint procedures
- Whether the provision of personal data is part of a statutory of contractual requirement or obligation and possible consequences for any failure to provide the data