# Data protection Policy

## 1. Introduction

ABG Limited needs to gather and use certain information about individuals.

These 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, handles and stored to meet the company's data protection standards and to comply with the law.

## 2. Why this policy exists

This data protection policy ensures ABG Limited:

- 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 individual's data.
- Protects itself from the risks of a data breach.

## 3. Data protection law

The Data Protection Act 1998 describes how organisations – including ABG Limited – must collect, handle and store personal information.

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 Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully.
2. Be obtained only for specific, lawful purposes.
3. Be adequate, relevant and not excessive.
4. Be accurate and kept up to date.
5. Not be held for any longer than necessary.
6. Processed in accordance with the rights of data subjects.
7. Be processed in appropriate ways.
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

## 4. People, risks and responsibilities

This policy applies to:

- The head office of ABG Limited.
- Any branches of ABG Limited.
- All staff of ABG Limited.
- All contractors, suppliers and other people working on behalf of ABG Limited.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:


**abg ltd.** E7 Meltham Mills Rd, Meltham, West Yorkshire, HD9 4DS
**UK t** 01484 852096 **e** geo@abgltd.com **Export t** +44(0)1484 852250 **e** export@abgltd.com
**www.abgltd.com**

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- ….plus any other information relating to individuals

## 9. Data protection risks

This policy helps to protect ABG Limited 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.

## 10. Responsibilities

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

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

However, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that ABG Limited meets its legal obligation.
- The [data protection officer}, Alek Jovetic, 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, if appropriate, 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.
  - Directing any requests from individuals to see the data ABG Limited holds about them (also called ‘subject access requests’) to HR Department.
- The [contracted IT manager], Ian Tattershall, 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.
- The [designated website manager], Jim Herbert, is responsible for:
  - Approving any data protection statement attached to communications such as emails and letters.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

## 11. General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.


**abg ltd.** E7 Meltham Mills Rd, Meltham, West Yorkshire, HD9 4DS
**UK t** 01484 852096 **e** geo@abgltd.com **Export t** +44(0)1484 852250 **e** export@abgltd.com
**www.abgltd.com**

- Data should not be shared informally. When access to confidential information is required, employees MUST request it from their line managers.
- ABG Limited will provide training, when appropriate, 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 should never be shared. If they are, they should be changed at the earliest opportunity.
- Personal data should not be disclosed to unauthorised people, either within the organisation or externally.
- Data should be regularly reviewed and updated if it is found to be incorrect. If no longer required, it should be deleted and correctly 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.

## 12. Data storage

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 protection 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 or copier.
- Data printouts should be shredded or disposed of securely when no longer required.

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

- Data should be protected by strong passwords and never shared between employees.
- If data is stored on removable media (like CD, DVD, memory stick), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers.
- Servers containing personal data should be sited in a secure location away from general office space.
- Data should be backed up frequently. These backups should be tested periodically in line with the company's standard back up and disaster recovery procedures.
- Data should never be saved directly to laptops or other devices like tablets or smart phones.
- All servers containing data should be protected by approved and adequate security software and a firewall.

## 13. Data use

Personal data is of no value to ABG Limited 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.


**abg ltd.** E7 Meltham Mills Rd, Meltham, West Yorkshire, HD9 4DS
**UK t** 01484 852096 **e** geo@abgltd.com **Export t** +44(0)1484 852250 **e** export@abgltd.com
**www.abgltd.com**

- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- In the rare event where sensitive data is being sent externally to a third party, it must be encrypted before being transferred electronically. The IT manager will be able to advise in such a situation.
- Personal data should never be transferred outside the European Economic Area.
- Employees should not save copies of personal data to their own devices. Always access and update the central copy of any data.

## 14. Data accuracy

The law requires ABG Limited 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 ABG Limited 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 if possible.
- ABG Limited will make it easy for data subjects to update the information ABG Limited holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, is a customer can no longer be reached on their stored number; it should be removed from the database.

## 15. Subject access requests

All individuals who are the subject of personal data held by ABG Limited 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'.

HR will validate these requests and aim to provide the relevant data within 30 days.

## 16. Disclosing data for other reasons

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

Under these circumstances, ABG Limited will disclose requested data. However, the data controller will have to be satisfied that the request is legitimate, seeking assistance from the board, or in extreme cases, the company's legal advisers.


**abg ltd.** E7 Meltham Mills Rd, Meltham, West Yorkshire, HD9 4DS
**UK t** 01484 852096 **e** geo@abgltd.com **Export t** +44(0)1484 852250 **e** export@abgltd.com
**www.abgltd.com**