Our Data Protection Policy

Introduction

DBS Datamarketing Limited needs to gather and process 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, handled and stored to meet the company's data protection standards and to comply with the law.

Why this policy exists

This data protection policy ensures DBS Datamarketing Limited:

- Complies with data protection law and follow 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 Data Protection Act (DPA), The Privacy and Electronic Communications Regulations (PECR), The General Data Protection Regulation (GDPR) and statutory codes issued by the Information Commissioner's Office (ICO), describe how organisations, including DBS Datamarketing Limited, must collect, process, 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 processed fairly, stored safely and not disclosed unlawfully.

The GDPR is underpinned by seven principles:

1. Lawfulness, fairness & transparency]
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity & confidentiality
7. Accountability

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

The DPA is underpinned by six principles to ensure that data is:

1. used fairly, lawfully and transparently
2. used for specified, explicit purposes
3. used in a way that is adequate, relevant and limited to only what is necessary
4. accurate and, where necessary, kept up to date
5. kept for no longer than is necessary
6. handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Best practice guidance & codes

We are committed to the highest possible levels of compliance, this means that we strive to exceed best practice defined by the Direct Marketing Association code (DMA), the ICO codes and guidance and our own ethical policy.

Policy scope

This policy applies to:

- The head office of DBS Datamarketing Limited
- All branches of DBS Datamarketing Limited
- All staff and volunteers of DBS Datamarketing Limited
- All contractors, suppliers and other people working on behalf of DBS Datamarketing 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 (DPA), The Privacy and Electronic Communications Regulations (PECR) and The General Data Protection Regulation (GDPR). This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

Data protection risks

This policy helps to protect DBS Datamarketing 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 processes 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 DBS Datamarketing Limited has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team 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 DBS Datamarketing Limited meets its legal obligations.

- The Data Protection Officer, 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.
  - Handling data protection questions from staff and anyone else covered by this policy.
  - Dealing with requests from individuals to see the data DBS Datamarketing Limited 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.

- The CTO 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, is responsible for:
  - Approving any data protection statements attached to communications such as emails and letters.
  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

- Data access is limited to employees whose roles are conditional upon it.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.

- DBS Datamarketing Limited 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, long and complex passwords must be used, regularly changed and 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.

Data storage & information security

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the CTO 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 DVD), 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 DBS Datamarketing Limited unless the business can demonstrate a clear benefit.

However, it is when personal data is accessed or shared 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 CTO 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 DBS Datamarketing 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 DBS Datamarketing 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.
- DBS Datamarketing Limited will make it easy for data subjects to update the information DBS Datamarketing Limited 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.

All individuals who are the subject of personal data held by DBS Datamarketing 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.

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

The data controller will aim to provide the relevant data within 7 days.

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

In certain circumstances, The Data Protection Act (DPA), The Privacy and Electronic Communications Regulations (PECR) and The General Data Protection Regulation (GDPR) allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, DBS Datamarketing Limited 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.

DBS Datamarketing Limited is committed to ensuring that individuals are aware that their data is being processed, and that they understand:

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

The company has a privacy policy and specific policies that govern each aspect of its data processing.

Updated 14th October 2021