



# Data

# Protection

# Policy

# Data protection policy

## Context and overview

### Key details

- |   |                       |
|---|-----------------------|
| <input type="checkbox"/> Policy prepared by:                | Avril James           |
| <input type="checkbox"/> Approved by board / management on: | Avril James 30-1-2018 |
| <input type="checkbox"/> Policy became operational on:      | 30-1-2018.            |
| <input type="checkbox"/> Next review date:                  | 25-3-2025             |

### Introduction

**Ask Avril** 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, 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 Ask Avril:

- ☐ 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 1998 describes how organisations — including **Ask Avril** 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 protected 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

## People, risks and responsibilities

### Policy scope

This policy applies to:

- ☐ The Virtual Assistant/Owner of Ask Avril
- ☐ All contractors, suppliers and other people working on behalf of **Ask Avril**

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:

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

### Data protection risks

This policy helps to protect Ask Avril 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 Ask Avril 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 **Owner/Virtual Assistant** is ultimately responsible for ensuring **that Ask Avril** meets its legal obligations.
- The **data protection officer, Avril James** is responsible for:
  - Keeping 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 **Ask Avril** 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.
  - Ensuring all systems, services and equipment used for storing data meets 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.
  - 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.

## General 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.
- **The owner/Virtual Assistant - Ask Avril will undertake any training** to help them understand their responsibilities when handling data.
- All data will be kept secure, Ask Avril will take all sensible precautions by following the guidelines below.
  - In particular, **strong passwords will be used** and never be shared.
  - Personal data **will not be disclosed** to unauthorised people, either within the company or externally.
  - Data will be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it will be deleted and disposed of.

## Data storage

When data is **stored on paper**, it will be kept in a secure place where unauthorised people cannot see it.

This also applies to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files will be kept **in a locked drawer or filing cabinet**.
- Ask Avril will ensure that paper and printouts are **not left where unauthorised people could see them**,
- **Data printouts will 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 will be **protected by strong passwords** that are changed regularly and never shared between employees.
- When data is **stored on removable media** (like a CD or DVD), these will be kept locked away securely when not being used.
- Data will only be stored on **designated drives and servers**, and will only be uploaded to an **approved cloud computing services**.
- Servers containing personal data will be **sited in a secure location**, away from general office space.
- Data will be **backed up frequently**. Those backups will be tested regularly, in line with the company's standard backup procedures.
- Data will **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data are protected by **approved security software and a firewall**.

## Data use

Personal data is of no value to Ask Avril 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, Ask Avril will ensure **the screens of their computers are always locked** when left unattended.
- Personal data **will not be shared informally**. In particular, it will never be sent by email, as this form of communication is not secure.
- Data will be **encrypted before being transferred electronically**.
- Personal data will **never be transferred outside of the European Economic Area**.
- **Personal data will not be saved on personal computers**  
Data will always be accessed and update on the central copy.

## Data accuracy

The law requires Ask Avril 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 Ask Avril should put into ensuring its accuracy.

It is the responsibility of Ask Avril when working 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**. Unnecessary additional data sets will not be created.
- Ask Avril will **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.
- Ask Avril will make it **easy for data subjects to update the information** Ask Avril holds about them. For instance, via the company website.
- Data will be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it will be removed from the database.
- Ask Avril will ensure **marketing databases are checked against industry suppression files** every six months.

## Subject access requests

All individuals who are the subject of personal data held by Ask Avril 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 **avril@askavril.co.uk**. The data controller can supply a standard request form, although individuals do not have to use this.

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

## 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, Ask Avril 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.

## Providing information

Ask Avril aims to ensure that individuals are aware that their data is being processed, and that they understand:

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

To these ends, 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.]