# General Data Protection Regulation policy

## Context and overview

### Introduction

Accuracy Matters Ltd needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees, freelance associates 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 General Data Protection Regulation (GDPR).

### Why this policy exists

This GDPR policy ensures that Accuracy Matters Ltd:

- complies with GDPR law and follows good practice
- protects the rights of staff, customers and associates
- is open about how it stores and processed individuals' data
- protects itself from the risks of a data breach.

### GDPR law

The GDPR forms part of the data protection regime in the UK, together with the Data Protection Act 2018. Together, this legislation describes how organisations – including Accuracy Matters Ltd – 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 GDPR is underpinned by seven important principles:

1. lawfulness, fairness and transparency
2. purpose limitation
3. data minimisation
4. accuracy
5. storage limitation
6. integrity and confidentiality (security)
7. accountability

These principles lie at the heart of our approach to processing personal data.

### Lawfulness, fairness and transparency

We always process personal information lawfully and fairly. We  are also open and honest with individuals about the data that we hold about them.

### Purpose limitation
We are clear from the outset why we collect personal data and explain what we will do with it. If we plan to use or disclose personal data for any purpose that is additional or different from the purpose we originally specified, we make sure that the new use is fair, lawful and transparent.

### Data minimisation
We only hold the minimum amount of personal data that we need. Individuals have the right to complete any incomplete data we hold about them, and they have the right to ask us to delete any data that is not necessary for our purposes.

### Accuracy
We take great care to delete or correct any inaccurate personal data. We also review the personal data we hold to ensure it remains up to date.

### Storage limitation
We only keep personal data for as long as we need it. We always review whether or not we still need to keep personal data if an individual asks us to delete it.

### Integrity and confidentiality (security)
We have robust security measures in place to ensure that personal data is secure.

### Accountability
We are accountable for how we treat personal data and take this role very seriously.

## People, risks and responsibilities

### Policy scope
This policy applies to:

- all staff and volunteers of Accuracy Matters Ltd
- all freelance associates (contractors, suppliers and other people) working on behalf of Accuracy Matters Ltd.

It applies to all data that the company holds relating to identifiable individuals. This can include:

- names of individuals
- postal addresses
- email addresses
- telephone numbers
- and any other information relating to individuals.

### Data protection risks
This policy helps to protect Accuracy Matters Ltd 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 Accuracy Matters Ltd has some responsibility for ensuring that 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, the Managing Director has the following key areas of responsibility:

- The Managing Director is ultimately responsible for ensuring that Accuracy Matters Ltd meets its legal obligations.
- Regarding overall data protection policy:
    - Keeping up to date about data protection responsibilities, risks and issues
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule
    - Handling data protection questions from staff and anyone else covered by this policy
    - Dealing with requests from individuals to see the data that Accuracy Matters Ltd 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.
- Regarding IT:
    - Ensuring that all systems, services and equipment used for storing data meet acceptable security standards
    - Performing regular checks and scans to ensure that 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.
- Regarding marketing activities:
    - 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 that marketing initiatives abide by data protection principles.

For any new projects involving processing of people's data that is **likely to result in a high risk to individuals**, the Managing Director must consider preparing a Data Protection Impact Assessment (a template DPIA is available on request from the Managing Director).

## 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 the Managing Director.
- 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 the Managing Director if they are unsure about any aspect of data protection.

## Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Managing Director.

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 that paper and printouts are **not left where unauthorised people could see them**, such as 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 **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 (see 4.2 IT systems, spec and security in the Operations Manual).
- Data should **never be saved directly** to laptops or other mobile devices such as tablets or smartphones.
- 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 Accuracy Matters Ltd 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 that **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 Managing Director can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the EEA**.
- 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 Accuracy Matters Ltd to take reasonable steps to ensure that data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Accuracy Matters Ltd should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure that 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 data sets.
- Staff should **take every opportunity to ensure that data is updated**. For instance, by confirming a customer's details when they call.
- Accuracy Matters Ltd will make it **easy for data subjects to update the information** Accuracy Matters Ltd 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.

## Subject access requests

All individuals who are the subject of personal data held by Accuracy Matters Ltd 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 Managing Director. The Managing Director can supply a standard request form, although individuals do not have to use this.

Individuals may be charged for the administrative costs of complying with a subject access request. The Managing Director will aim to provide the relevant data within one calendar month.

The Managing Director 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, Accuracy Matters Ltd will disclose requested data. However, the Managing Director will ensure that the request is legitimate, seeking assistance from the company's legal advisers where necessary.

## Providing information

Accuracy Matters Ltd 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 (Operations Manual 3.B6), 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