

# ARC:MC Policy Data protection/GDPR policy

## Context and Overview

### Introduction

ARCMC needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts and other people the business 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 ARC:MC:

- Complies with data protection law and follows good practice
- Protects the rights of customers, suppliers and business contacts
- 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 ARC:MC— 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 main office of ARC:MC
- All contractors, suppliers and other people working on behalf of ARC:MC

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 ARC:MC 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 ARC:MC has some responsibility for ensuring data is collected, stored and handled appropriately. They must ensure that it is handled and processed in line with this policy and data protection principles.

The key areas of responsibility:

Reviewing all data protection procedures and related policies, in line with an agreed schedule.

Handling data protection questions from anyone covered by this policy.

Dealing with requests from individuals to see the data ARC:MC 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 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.

#### General Contractor 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.
- Contractors 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.
- Contractors should request help from ARC:MC 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 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.
- Contractors 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.
- 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.
- Data should be backed up frequently. Those backups should be tested regularly.
- 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 ARC:MC 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, Contractors should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally.
- Personal data should never be transferred outside of the European Economic Area.
- Contractors 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 ARC:MC 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 ARC:MC should put into ensuring its accuracy.

It is the responsibility of all contractors 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.
- ARC:MC will make it easy for data subjects to update the information held about them.
- 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 ARC:MC 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 [stuart.camoccio@arcmc.co.uk](mailto:stuart.camoccio@arcmc.co.uk)

Individuals will be charged £10 + VAT per subject access request. The data controller will aim to provide the relevant data within 21 days.

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, ARC:MC will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the company's legal advisers where necessary.