

# Data Protection Policy

## Introduction

Sometimes RG Jones need to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, staff 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 how the company:

- Complies with GDPR 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 General Data Protection Regulation (GDPR) is a new European Union (EU) privacy law that takes effect on May 25, 2018. It is designed to give individuals control over their personal data and is an important effort for protecting individual rights and freedoms.

The GDPR applies to any Organisations based in the EU and Organisations—wherever they are located—that are selling goods and services in the EU or processing personal data of individuals in the EU.

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

Article 5 of the GDPR requires that personal data shall be:

- “a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

# People, risks and responsibilities

## Policy scope

This policy applies to RG Jones.

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

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- ...plus any other information relating to individuals
- Client information
- Contracts
- Staff information including payroll, benefits, Right to Work and passports

## Data protection risks

This policy helps to protect RG Jones 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 us 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:

- **Andrew Williamson** is ultimately responsible for ensuring that the company meets its legal obligations.

**Andrew Williamson** is responsible for:

- Keeping all staff 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 that the company 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.

## 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 their line managers.
- **The company 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 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 their line manager 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 their line manager.

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**.
- Staff 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**.
- Access rights to data should be regularly reviewed

## Data use

Personal data is of no value to the company 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, staff 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, unless it is password protected.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.
- **Staff 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 us 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 the company should put into ensuring its accuracy.

It is the responsibility of all staff 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**.
- The company will make it **easy for data subjects to update the information** we hold about them. For instance, via the Subject Access Request Policy.
- 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 the company 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 [info@rgjones.co.uk](mailto:info@rgjones.co.uk)

Individuals will not be charged for subject access requests. The company will aim to provide the relevant data within 30 days.

The company 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, GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, RG Jones will disclose requested data.



# Providing information

The company 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.