

# ROBINSON REED LAYTON LLP

## Data Protection Policy

### Introduction

Robinson Reed Layton LLP needs to gather and use certain information about individuals.

These can include customers, suppliers, business contact, 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.

Personal data means data held either on a computer or in a paper-based filing system which relates to a living individual who can be identified from that data.

### Why this policy exists

This data protection policy ensures Robinson Reed Layton LLP:

- Complies with General Data Protection Regulations 2018 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 2018 (GDPR) describes how organisations – including Robinson Reed Layton LLP – 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 General Data Protection Act 2018 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. Be processed in accordance with the rights of data subjects.
7. Be protected in appropriate ways.
8. Not to 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 head office of Robinson Reed Layton LLP.
- All branches of Robinson Reed Layton LLP.

- All staff of ROBINSON REED LAYTON LLP.

All contractors, suppliers and other people working on behalf of Robinson Reed Layton LLP. It applies to all personal data that the company holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulations 2018. This can include:

- Names of individuals.
- Postal addresses.
- Telephone numbers

Plus any other information relating to individuals.

### **Data Protection Risks**

This policy helps to protect Robinson Reed Layton LLP and our clients 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 where possible 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 Robinson Reed Layton LLP 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 Partners are ultimately responsible for ensuring that Robinson Reed Layton LLP meets its legal obligations.
- The Data Controller, is responsible for:
  - Keeping the Partners 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 Robinson Reed Layton LLP holds about them (also called 'subject access request').
  - Dealing with and reporting data breaches.
  - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- The Office Manager, 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 Office 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.

### **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.
- Robinson Reed Layton LLP 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 or the Data Controller 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 Office 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.
- 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 USB), 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 service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- 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 Robinson Reed Layton LLP 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 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 Office Manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area unless specific criteria are met.
- 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 Robinson Reed Layton LLP 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 Robinson Reed Layton LLP 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.
- Robinson Reed Layton LLP will make it easy for data subjects to update the information Robinson Reed Layton LLP holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a client can no longer be reached on their stored telephone number, it should be removed from the database.

### **Subject Access Requests (SARs)**

All individuals who are the subject of personal data held by Robinson Reed Layton LLP are entitled to:

- Have confirmed that the company is processing their data
- 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 [michelle.pearce@rrlcornwall.co.uk](mailto:michelle.pearce@rrlcornwall.co.uk).

We do not routinely charge a fee for Subject Access Requests. The General Data Protection Act 2018 requires that a full response must be sent within one calendar month starting from the date when we received all the information necessary to identify you and identify the information requested. We will aim to respond to all requests as soon as possible within this timeframe.

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 General Data Protection Act 2018 allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Robinson Reed Layton LLP 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**

Robinson Reed Layton LLP 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.