Data Management Policy

June 2024

Version 1.0

Contents

Document control

Version	Date	Author	Amendment
1.0	June 2024	Terri Pugh	Creation

Distribution list

This document has been distributed to all employees at R.J. Francis & Co. Limited (RJF).

Introduction

The Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR) requires organisations that process personal data to meet certain legal obligations. RJF are a data controller within the meaning of the Act and we process personal data.

We are committed to complying with the requirements of the DPA and GDPR. As a result we confirm that personal information we process will only be held (or otherwise processed) to the extent necessary in order to provide the agreed professional services and for any other purpose specifically agreed.

RJF needs to gather and use certain information about individuals. This can include clients, contacts, employees and other people the organisation has a relationship with or may need to contact.

This Data Management Policy sets out the requirements for the following, in line with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

- How documents and records are collected, handled and stored
- Document retention periods
- Disposal of documents and records after the end of the retention period

Details of any individual variations to the documented retention periods will be documented and retained on the client records, and will override this policy.

This policy ensures that RJF complies with data protection law and follows good practice, protects the rights of clients, employees and partners, is transparent about how it processes individuals' data, and protects itself from the risks of a data breach.

Data protection law

The UK General Data Protection Regulation (GDPR) applies in the UK. It outlines that personal data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. 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 or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. Adequate, relevant and limited to what's necessary in relation to the purposes for which they're processed.
4. Accurate and, where necessary, kept up to date.
5. Protected – every reasonable step must be taken to ensure that personal data that's inaccurate, having regard to the purposes for which they're processed, is erased or rectified without delay.
6. Kept in a form that permits identification of data subjects for no longer than is necessary, and for the purposes for which the personal data is processed (personal).
7. Stored for longer periods. For example, the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. This will also be subject to implementation of the appropriate technical and organisational measures required by UK GDPR in order to safeguard the rights and freedoms of individuals.
8. Processed in a manner that ensures appropriate security of personal data. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
9. Managed by a controller responsible for, and be able to demonstrate, compliance with the principles.

Responsibilities

Everyone at RJF contributes to compliance with UK GDPR.

The Data Protection Officer (DPO), responsible for ensuring that data protection requirements are met for RJF, is Andrew Houston.

The Compliance Officer (CO) for RJF may take the lead on embedding ongoing privacy measures into policies and day-to-day activities throughout the organisation, arranging training and advice for employees, and dealing with subject access requests, deletion requests and queries from clients, stakeholders and data subjects about data protection related matters.

Scope and use of personal information processed

Information collected

We need to collect, retain and process personal data. This data is needed in order to:

- Take on and retain a client according to the provisions of UK laws and professional regulations (e.g. anti-money laundering requirements)
- Prepare and file accounts and tax returns
- Provide advice on tax and national insurance liabilities
- Provide ad hoc advice
- Provide information about other services we provide which may be of interest
- Meet other legal and regulatory requirements

If the information required is not provided, we may not be able to provide the required services. The personal data that we may collect and process will include:

- Names
- Postal addresses
- Email addresses
- Telephone numbers
- Information held by HMRC
- Bank details
- Equality and diversity information
- Results of background checks
- Correspondence between us

Sources of information

We collect information that is supplied from:

- The individual
- A spouse/partner
- Your organisation
- HMRC
- Electronic ID verification providers
- Other third parties as authorised by you

There is no automated decision-making involved in the use of information held, and therefore no automatic data portability.

Where we use subcontractors they will comply with General Data Protection Regulation (GDPR) requirements.

Lawful basis for processing personal data

Personal data may be processed:

- On a contract basis under the engagement letter and provision of services agreements.
- On a consent basis when meeting wider expectations of our professional relationship.
- On the legal obligations and/or public interest bases in order to comply with legal requirements.
- In order to further our legitimate interests.

Privacy notices

RJF aims to ensure that individuals are aware that their data is being processed. The company has a privacy statement, setting out how data relating to these individuals is used by the company. This privacy statement can be found within the Letter of Engagement, on the RJF website, and a copy can be requested at any time.

Consent

A client's letter of engagement gives consent for the processing of information in line with this policy. The supply of information thereafter confirms ongoing permission to process information. Should the services we provide or the terms of our privacy notice change we will issue a new letter of engagement for approval.

Restrictions on processing (the right to restrict processing and the right to object)

In certain circumstances an individual has the right to 'block' or suppress the processing of personal data or to object to the processing of that information. Further information can be found on the ICO website (www.ico.org.uk). The individual should inform us immediately if they want us to cease processing their information or object to processing so that we can take the appropriate action.

Withdrawal of Consent

Where there is consent for us to contact an individual with details of other services we provide we may continue to process data and contact them for that purpose after our contractual relationship ends. They may withdraw consent for the firm to contact them in relation to details of other services we provide at any time during the performance of the contract or thereafter. The individual may do this in writing, by letter or by email. We will then cease to process data but only in connection with details of other services we provide. The withdrawal of consent does not make the other bases on which we are processing data unlawful. We will therefore still continue to process data under the terms of our contract and for other reasons set out in this privacy notice.

Retention of documents and records

Paper documents and records

While an individual remains an active client, any hard copies of documents and records will be retained in dedicated folders. Folders will be created for each of the following entities:

- Limited company
- Sole trader
- Partnership
- Individual

Documents should be stored in the correct respective folder. For example, where there is an individual folder for a director of a limited company, paperwork regarding that director should be stored in their individual folder, and not within the limited company folder, unless it specifically relates to their activity within the limited company.

These folders will be stored in a records room.

Any client information supplied to RJF by the client for the purpose of services being fulfilled will be stored in the original container they were delivered in, also in a records room. Original documents will be returned to the client on completion of the relevant services, however RJF may retain copies where appropriate.

Documents will be temporarily relocated to a staff member's workspace only for the duration required to complete the task, after which they will be returned to their storage location. Staff will diligently ensure that documents are handled discreetly while in use, and that they will be kept out of unauthorised view.

Should services terminate, we will make every effort to return any client owned documents. Any remaining information and folders relating to that client may be retrieved from the records room and moved to archiving at our local external secure storage facility.

Electronic documents and records

Electronic copies of documents and records will be retained in electronic folders. These folders will be stored on a secure server, within RJF premises. Data is backed up to portable drives daily.

Data may be stored within licenced third party software.

Should our professional relationship terminate, documents and records relating to that individual will remain on our server for the acceptable retention period.

Electronic documents retrieved to complete a task will be handled with sensitivity. They will be open for as long as is necessary to complete the task, and not unnecessarily duplicated for storage outside of the main folder.

All staff members must lock their computers when stepping away from their desks to prevent unauthorised access to data.

Retention periods

RJF retention periods are as follows:

Client data

Type of document	Minimum Retention period
Anti-money laundering records	Throughout the period of the relationship but deleted 7 years after the end of the business relationship
Accounts preparation working papers Ad hoc advisory work records Assurance files Audit files General correspondence and other office papers Insolvency files PAYE files Tax papers – income tax, capital gains tax, corporation tax, VAT	Current financial year plus 6 further years
Client records relating to pension transfers and opt-outs	Indefinitely
Information relating to a client's chargeable assets and gifts	Indefinitely
Investment business records	6 years from document creation date
Title documents	12 years after end of interest in property

Additionally, where we have received (or has been notified of) a complaint, claim or inquiry, or foresee that happening, we reserve the right to extend the retention periods as necessary.

Deleting records (the right to erasure)

In certain circumstances it is possible for an individual to request the erasure of their records before the end of the retention periods. Further information is available on the ICO website (www.ico.org.uk). If someone would like their records to be erased, they should inform us immediately and we will consider their request. In certain circumstances we have the right to refuse to comply with a request for erasure and if applicable we will respond with the reasons for refusing the request.

Disposal of documents and records

Any documents and records still held after the required retention period will be subject to secure disposal.

Paper documents and records

RJF employs the services of a third party confidential waste management company, Yeomans Storage Limited (YSL). Any documentation due for disposal is collected by this company and securely destroyed on our behalf. A Confidential Destruction Advice is supplied by YSL for each collection of papers to be destroyed.

Electronic documents and records

Care is taken to remove all electronic documents and records from RJF and third party systems and software. Data is removed from live data sources at the earliest opportunity.

Data may remain on RJF backup drives for up to 90 days. After this time they will be automatically overwritten. However, this backup data can be deleted sooner at the request of the client.

Client owned documents and records

These records are retained for as long as is necessary to fulfil the purposes for which it is collected. After this time RJF will make every effort to return all client owned documents to the client, in line with the RJF Return Of Client Records procedure, before final disposal.

Data sharing

In order for us to provide the agreed services, we may provide personal data about an individual to:

- HMRC
- Other third parties we are required to correspond with, for example, finance providers, pension providers (including auto-enrolment) and investment brokers.
- Subcontractors who are bound by the same professional and ethical obligations as the principals and employees of the practice
- An alternate party appointed by us in the event of incapacity or death. Details of the name and address of this individual will be provided on request.
- Tax insurance providers
- Professional indemnity insurers
- Our professional body, the Institute of Chartered Accountants in England and Wales (ICAEW), or an external reviewer in relation to quality assurance.

We need to give information to these other parties in order to fulfil our contractual obligations to individuals and therefore it is not possible to opt out of the provision of information to these parties. If we are asked not to provide information we may need to cease to act.

If the law allows or requires during the period of our contractual arrangements or after we have ceased to act we may give information about you to:

- The police and law enforcement agencies
- Courts and tribunals
- The Information Commissioner's Office (ICO).

In addition, after we have ceased to act we may give information about you to:

- Our professional indemnity insurers or legal advisers where we need to defend ourselves against a claim
- Our professional disciplinary body where a complaint has been made against us in order to defend ourselves against a claim
- New agents, advisers, or other third parties that a client asks us to give information to

Transferring of data

We will communicate or transfer data using any of the following methods:

- Post/hard-copy documents
- Password-protected emails
- Encrypted emails
- Unencrypted emails (without attachments)
- Secure portals
- Cloud-based software

Wherever possible our preferred method of communication and document sharing is electronic documents, via OpenSpace, our secure client portal.

Where this is unacceptable to the client, sensitive data will only be transmitted electronically using password protected and encrypted emails. Any password must be sent in a separate email to that containing the data.

Where the mailing of hard copies is required, documents will be sent using a tracked and signed for mailing service.

An individual accepts the risks of corresponding with RJF using a delivery service that is not our secure portal. Written confirmation will be required.

We will not transfer the personal data outside of the UK.

Obtaining and reusing personal data (the right to data portability)

The right to data portability only applies:

- To personal data an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract, and
- When processing is carried out by automated means

An individual may be able to request their personal data in a format which enables it to be provided to another organisation. We will respond to any requests made without undue delay and within one month. We may extend the period by a further two months where the request is complex or a number of requests are received, but we will inform the person within one month of the receipt of the request and explain why the extension is necessary.

Data security

Data is backed up to three portable drives; two of which remain on the premises and one is taken off site in case of an incident which may cause damage to the IT equipment, such as a fire or lightning strike. The portable drive taken off site is transported safely and directly to the off site location, where it is stored in a moderately cool temperature, away from humidity, shocks and static. It will at all times remain out of site, and stored in a secure place with no access by others.

RJF employs an external company, Hereford Computer Services (HCS), to provide IT support within the business. HCS has provided us with a Privacy Policy, detailing how they manage our data. No internal data from our servers is held by HCS.

HCS are responsible for ensuring that measures like security software and firewalls, encryption, the use of secure Virtual Private Networks (VPN), software updates, log-in restricted access and two step authentications, are in place where appropriate.

We have put in place additional appropriate and proportionate security measures to address the risk of personal data being lost, used, altered or accessed in an unauthorised way. We limit access to personal data to those who have a business need to access it, and who will only process the personal data on our instructions.

Nevertheless, no data transmission over the internet, or any other network, can ever be regarded as wholly secure, and we have in place measures to deal with any suspected breach of data security. Those measures include policies and procedures, which are periodically reviewed to ensure they are effective and fit for purpose.

RJF has a standalone Data Breach Reporting Procedure which can be actioned in the instance of a known data breach, to ensure reporting to the ICO is within the required timescales.

Subject access requests

All individuals who are the subject of data held by our organisation 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

Requests to see records and other related information that the firm holds about an individual are known as 'subject access requests' (SAR). All requests should be made in writing to the DPO.

Copies of identification and proof of address may be requested before the SAR can be actioned.

RJF has one month in which to respond to a SAR. If the information is complex and we are unable to provide the information in this time we may extend the response time by up to two months. We will inform the individual if this happens.

Asking someone else to make a subject access request on your behalf

An individual can ask someone else to request information on their behalf – for example, a friend, relative or solicitor. We must have written authority to do this. This is usually a letter signed by the individual stating that they authorise the person concerned to ask for information, and/or receive our reply.

When we won't release information

The law allows us to refuse a request for information in certain circumstances – for example, if a similar request has previously been made and there has been little or no change to the data since the original request.

The law also allows us to withhold information where, for example, release would be likely to:

- Prejudice the prevention or detection of crime
- Prejudice the apprehension (arrest) or prosecution of offenders
- Prejudice the assessment or collection of any tax or duty
- Reveal the identity of another person, or information about them.

Where we are unable to consent to a request we will set out the reasons in writing.

Putting things right (the right to rectification)

Should information previously supplied to us be incorrect, we should be informed immediately so we can update and amend the information we hold.

Complaints

If any person has questions or concerns regarding our processing of personal data, they can complain to us as set out in the RJF Complaints Policy & Procedure.

If they are dissatisfied with the response, then they can refer to the ICO. Details can be found at www.ico.org.uk.

The person can also complain to our professional body – the Institute of Chartered Accountants in England and Wales (ICAEW). Their details can be found at www.icaew.com.