General Data Protection Regulation: Records of processing activities

6 March 2024

DORE FINANCIAL LIMITED

(Supervisory Authority Reference:)	Address: 85 SINCLAIR ROAD LONDON W14 0NR
Phone: 02030 166901	Email: timc@dorefinancial.co.uk

Data Protection Officer: Timothy Couldwell

	Address: 85 Sinclair Road London W14 0NR
Phone: 0203 166901	Email: timc@dorefinancial.co.uk

Internal Organisational Policies

Complaints Procedure Policy	
Data Destruction / Retention Policy	
Data Protection Policy	
Data Transfer Policy	
Information Security Policy	
Mobile Working Policy	
Outsourcing Policy	
Privacy Policy	
Records Management Policy	

Organisational Wide Measures

Pseudo-Anonymisation is used where possible.	Personal data cannot be linked back to an identifiable individual wherever possible.
Backups are automated.	Personal data is backed up securely to ensure it can be recovered in the event of system failures. Where possible data is encrypted.
Paper based files are handled securely.	Your business stores paper and electronic records securely with appropriate environmental controls and higher levels of security around sensitive personal data. Your business restricts access to records storage areas in order to prevent unauthorised access, damage, theft or loss. Access should be role based in line with the principle of least privilege and checked regularly.
Paper files are shredded when no longer needed.	Paper files no longer needed by the business are securely destroyed by on-site shredding using a reputable company under contract or the firms own shredding machine.
Backups are encrypted before transferring to third party servers.	Data is encrypted befor moving it to an external site. This adds extra security to data should the third party site suffer a data breach.
Data is accurate and kept up to date.	Your business has established processes to ensure personal data is of sufficient quality to make decisions about individuals (eg annual fact find updates).
Data is destroyed when it is no longer required.	Your business has established a process to routinely dispose of personal data that is no longer required in line with agreed timescales.
Encryption is used on portable devices.	All personal data on portable devices (eg. laptops, backup drives, tablets, phones) is 'scrambled' using encryption so that it cannot be read by unauthorised people.
Disable USB & CD Drives to prevent data harvesting or introduction of a virus.	Office desktops have a removable media block policy enforced to help prevent data loss and mitigate risk to the IT network.

Securely remove all personal information before disposing of old computers.	Data is removed either by destroying the computer hard disk or by using software.
Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected.	Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected.
Equipment holding personal data is secured.	Your business has established a process to configure new and existing hardware to reduce vulnerabilities and provide only the functionality and services required.
There is a strong password protection policy.	Access to personal data is prevented by ensuring systems only allow the implemtation of secure password policies. Mobile devices (ncluding mobile phones) have appropriate PINS or passwords.
There is a suitably configured firewall in place.	A firewall has been installed to protect the network from unauthorised access. The configuration has been carried out by a qualified engineer.
Secure connections are implemented.	The use of TLS to prevent unauthorised disclosure of personal data.
System blocking of certain websites.	Systems automatically bock websites which may pose a threat to internal systems.
Email encryption is deployed.	Systems automatically protect emailed documents and offer encryption to protect unauthorised disclosure.
Software patches and updates are applied in a timely manner.	Software is updated in a controlled and planned way to ensure systems are secure and prevent accidental loss or damage.
Timeout screen locks implemented.	Systems automatically lock after a period of inactivity to prevent unauthorised access to personal data.
Role-based access controls implement least privilidge.	Staff are only given access to the least number of areas within systems and the network that are necessary to their role within the company.
Origo Unipass has been implemented.	Unipass helpes to provide further security when accessing systems.
Managers control system access.	Access to systems are only granted following agreement from managers confirming the requirement in relation to the purpose of processing.
Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery.	When posting sensitive persoanl data, Royal Mail special delivery is used to ensure appropriate security and tracking is in place.
Appropriate policies have been adopted.	Appropriate policies have been adopted and reviewed regularly to ensure data protection is addressed throughout all data processing stages. Policies and compliance are audited as appropriate.
High risk processes are documented.	Processes are identified and evaluated in relation to the risk they pose to data subjects. Those processes which pose a high risk to the rights and freedoms aof data subjets are documented.
Staff are trained in data protection requirments.	Staff receive initial and ongoing training and awareness about data protection issues. Staff understand the firm's responsibilities when processing personal data and receive relevant reminders about key areas of risk. This 'when' and 'what' training can be evidenced.
The firm undergoes data protection audits.	Policies are reviewed and compliance with these and relevant legisaltion can evidenced.
Due diligence is carried out on third parties.	Data is not shared with third parties unless there is a suitable written contract in place. Data is not shared with international organisations unless they have passed EU due diligence and adequacy requirements.
The ICO website is regularly accessed or the firm subscribes to the ICO newsletter.	The ICO website and newsletter provides a wealth of practical advice and explanation.
Staff have appropriate background checks.	Background checks such as DBS or previous employer references are obtained as a condition of employment.
There is a contact point for data subjects.	Data subjects know who to contact to raise a complaint, update their personal information or exercise any of their rights.
A data protection officer has been appointed.	Appointing a Data Protection Officer is one of the ways you can ensure the organisation works towards a culture of data protection.
The data protection officer is involved properly and in a timely manner in all issues which relate to data protection.	The Data Protection Officer is involved properly and in a timely manner in all issues which relate to data protection ensures the organisation gives due regard to its data protection responsibilities to data subjects.
Personal data breaches are reported to the Data protection officer.	Personal data breaches are reported to the data protection officer to ensure the organisation takes appropriate action to contain, mitigate and report a breach.
When engaging the services of another party to process data, an appropriate written contract protecting the rights and freedoms of data subjects is always put in place before any data are transferred.	Contracts ensure that action can be taken by the data controller to uphold the rights of data subjects.
When jointly processing data with another controller, the responsibilities and the essence of any contract are clear and made available to data subjects.	Contracts ensure that action can be taken by the data controller to uphold the rights of data subjects.

Subject access requests procedure implemented.	Your business has established a process to recognise and respond to individuals' requests to access their personal data.
Data protection impact assessments are carried out.	Your business has established a process to ensure new projects or initiatives are privacy-proofed at the planning stage. Data protection impact assessments are carried out and due regard is given to the risk associated with processing operations.
Risk management procees is in place.	Your business has established a process to identify, assess and manage information security risks. Your business ensures information security risks are assessed and appropriately managed.
A Business Continuity Plan is in place.	Your business has business continuity plans in place. These should identify business critical records that are essential to the continued functioning or reconstitution of the organisation in the event of a disaster. Data that is stored electronically should be routinely backed-up to help restore information in the event of disaster.
Data sharing is appropriate.	Your business maintains a log of all decisions to share personal data and this is reviewed regularly. Your business has agreed data sharing agreements with an appropriate legal basis with all parties with whom personal data is routinely shared or where large quantities of data are to be transferred. These agreements are regularly reviewed. Your business informs individuals about the sharing of their personal data.
Our website complies with cookie rules.	Your business has made privacy notices readily available to individuals.
Portable devices are kept locked away out of sight.	Portable devices pose a risk of theft or loss and are appropriately secured.
An appropriate cloud based service is used to store backups.	Data backups are stored securely and loss is prevented.
Antivirus and Malware protection are present on all PC's.	Software is installed to ensure systems are protected against unauthoried access, damage or data loss from viruses or malware.
Data search facilities are available.	Systems contain search facilities to enable personal data to be identified so that it may be updated, corrected, sent to the data subject or deleted as appropriate.
Network monitor software installed.	Software which detects unusual or malicious activity.
Email filtering of attachments.	Emails are filtered to reject or quarantine those with harmful attachments.
TPS/CTPS is consulted prior to marketing calls.	Individuals are not telephoned when they are registered with the telphone preference service. Your business identifies itself when making marketing phone calls.
Marketing lists only target individuals expecting contact from the firm.	Appropriate consent or legality for direct marketing can be evidenced. Marketing to individuals is only carried out when the individual is expecting this firm to contact them. Your business identifies itself when sending electronic marketing messages and ensures the initial and ongoing permission of recipients

Purposes of Processing Data by Process

Fact Find	To gather information about a client prior to and during a contract for services.
Client ID, Money Laundering, PEP and Sanction Checks	To verify the identity of the client, validate if they qualify as a PEP and ensure they are not included on the UK HM Treasury's sanction list.
Pension & Investment Product Research	To research the market for suitable products which match a clients needs and attitude to risk.
Product Application Processing	To prepare and submit an application on behalf of a client to a product provider.
Submission of Business Transactions to Regulated Principal	The firm submits business transactions to out regulated Principal to enable them to check compliance and process payment of adviser charges and/or commission.
Protection Annuity Quotation	To research the market for suitable products which match a clients needs and attitude to risk.

Fact Find

Purpose of Process	To gather information about a client prior to and during a contract for services.
Process Description	A financial adviser will collect information from the client to demonstrate 'know your client' using a fact find form. Information is collected using paper forms or laptops. Information is kept for as long as a relationship with the client exists and beyond that in line with the FCA's record keeping rules.

Data Subject	Data Category	Data Type
Customers / Clients	Personal data (non sensitive)	Name Nationality Pension details Life insurance details Investment details Employment details Mortgage details Information about a partner Information about dependents Assets and property information Tax information Information about credit status Information about marital status Information about age (eg date of birth)

Legal Basis for processing each category of data

Personal data (non sensitive)	The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Data Update Methods

UpdateMethod:	We rely on the data subject to inform us of changes.

Source of the Data

The Data Subject	
A Publically Available List	
Telephone conversations	
Emails or letters	

Categories of Data Recipient

Data Recipients:	Restricted staff, Contractors and agents

Data Retention and Disposal

Retention Time:	Indefinitely
Disposal:	FCA record keeping requirements

Protection Measures

Measures	Pseudo-Anonymisation is used where possible. Backups are automated. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Disable USB & CD Drives to prevent data harvesting or introduction of a virus. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a strong password protection policy. There is a suitably configured firewall in place. Secure connections are implemented. System blocking of certain websites. Email encryption is deployed. Software patches and updates are applied in a timely manner. Timeout screen locks implemented. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. The firm undergoes data protection audits. Due diligence is carried out on third parties. The ICO website is regularly accessed or the firm subscribes to the ICO newsletter. Staff have appropriate background checks. There is a contact point for data subjects. A data protection officer has been appointed. The data protection officer is involved properly and in a timely manner in all issues which relate to data protection. Personal data breaches are reported to the Data protection officer. When engaging the services of another party to process data, an appropriate written contract protecting the rights and freedoms of data subjects is always put in place before any data are transferred. When jointly processing data with another controller, the responsibilities and the essence of any contract are clear and made available to data subjects. Subject access requests procedure implemented. Data protection impact assessments are carried out. Risk management procees is in place. A Business Continuity Plan is in place. Data sharing is appropriate. Our website complies with cookie rules. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. Data search facilities are available. Network monitor software installed. Email filtering of attachments. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.
Data Storage	
Storage	Paper based. Local hard drive. Local server. Hosted servers. Cloud servers. Disk backups. Desk / Filing Cabinet. Laptop or portable device.

Fact Find: Risks & mitigating protection measures

Identity theft	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Staff have appropriate background checks. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.

Financial loss	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Staff have appropriate background checks. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Discrimination or unfair treatment	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Fraud	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Staff have appropriate background checks. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.

Damage to reputation	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Loss of confidentiality of data protected by professional secrecy	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Disable USB & CD Drives to prevent data harvesting or introduction of a virus. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a strong password protection policy. There is a suitably configured firewall in place. Email encryption is deployed. Software patches and updates are applied in a timely manner. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.

Loss of control of their data	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Disable USB & CD Drives to prevent data harvesting or introduction of a virus. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Software patches and updates are applied in a timely manner. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Subject access requests procedure implemented. Data protection impact assessments are carried out. Risk management procees is in place. A Business Continuity Plan is in place. Data sharing is appropriate. Our website complies with cookie rules. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. Data search facilities are available. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.
Limitation of their rights	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a strong password protection policy. There is a suitably configured firewall in place. Email encryption is deployed. Software patches and updates are applied in a timely manner. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Subject access requests procedure implemented. Data protection impact assessments are carried out. Risk management procees is in place. A Business Continuity Plan is in place. Data sharing is appropriate. Our website complies with cookie rules. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. Data search facilities are available.

Economic disadvantage	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Social disadvantage	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Causes distress to an individual	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.

May affect an individual's health, well-being or peace of mind	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.

Client ID, Money Laundering, PEP and Sanction Checks

Purpose of Process	To verify the identity of the client, validate if they qualify as a PEP and ensure they are not included on the UK HM Treasury's sanction list.
Process Description	Minimal information is passed into a third party system. The results returned then indicate if client is subject to any sanctions, is a PEP or if there are any issues validating their identity. The third party may keep a record of the information and may disclose the fact that a search of its records was made to its other customers for the purposes of assessing the risk of giving credit, to prevent fraud and to trace debtors. Our clients are notified of this fact via our privacy notice.

Data Subject	Data Category	Data Type
Customers / Clients	Personal data (non sensitive)	Name Address Telephone Numbers Passport Utility bill Information about gender

Legal Basis for processing each category of data

Personal data (non sensitive)	The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Further information about the legal basis for processing

The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	Processing of personal data which is necessary for the purposes of making a disclosure in good faith under section 21CA of the Terrorism Act 2000 (terrorist financing and identifying terrorist property) or section 339ZB of the Proceeds of Crime Act 2002 (money laundering).

Data Update Methods

UpdateMethod:	We rely on the data subject to inform us of changes. We periodically check with the data subject the accuracy of the personal data we hold.

Source of the Data

The Data Subject	

Categories of Data Recipient

Data Recipients:	Restricted staff

Data Retention and Disposal

Retention Time:	Indefinitely
Disposal:	FCA record keeping requirements

Protection Measures

Measures	Pseudo-Anonymisation is used where possible. Backups are automated. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Disable USB & CD Drives to prevent data harvesting or introduction of a virus. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a strong password protection policy. There is a suitably configured firewall in place. Secure connections are implemented. System blocking of certain websites. Email encryption is deployed. Software patches and updates are applied in a timely manner. Timeout screen locks implemented. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. The firm undergoes data protection audits. Due diligence is carried out on third parties. The ICO website is regularly accessed or the firm subscribes to the ICO newsletter. Staff have appropriate background checks. There is a contact point for data subjects. A data protection officer has been appointed. The data protection officer is involved properly and in a timely manner in all issues which relate to data protection. Personal data breaches are reported to the Data protection officer. When engaging the services of another party to process data, an appropriate written contract protecting the rights and freedoms of data subjects is always put in place before any data are transferred. When jointly processing data with another controller, the responsibilities and the essence of any contract are clear and made available to data subjects. Subject access requests procedure implemented. Data protection impact assessments are carried out. Risk management procees is in place. A Business Continuity Plan is in place. Data sharing is appropriate. Our website complies with cookie rules. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. Data search facilities are available. Network monitor software installed. Email filtering of attachments. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.
Data Storage	
Storage	Local hard drive. Local server. Hosted servers. Disk backups.

Client ID, Money Laundering, PEP and Sanction Checks: Risks & mitigating protection measures	
Identity theft	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Staff have appropriate background checks. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.

Financial loss	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Staff have appropriate background checks. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Discrimination or unfair treatment	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Fraud	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Staff have appropriate background checks. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.

Damage to reputation	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Loss of confidentiality of data protected by professional secrecy	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Disable USB & CD Drives to prevent data harvesting or introduction of a virus. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a strong password protection policy. There is a suitably configured firewall in place. Email encryption is deployed. Software patches and updates are applied in a timely manner. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.

Loss of control of their data	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Disable USB & CD Drives to prevent data harvesting or introduction of a virus. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Software patches and updates are applied in a timely manner. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Subject access requests procedure implemented. Data protection impact assessments are carried out. Risk management procees is in place. A Business Continuity Plan is in place. Data sharing is appropriate. Our website complies with cookie rules. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. Data search facilities are available. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.
Limitation of their rights	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a strong password protection policy. There is a suitably configured firewall in place. Email encryption is deployed. Software patches and updates are applied in a timely manner. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Subject access requests procedure implemented. Data protection impact assessments are carried out. Risk management procees is in place. A Business Continuity Plan is in place. Data sharing is appropriate. Our website complies with cookie rules. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. Data search facilities are available.

Economic disadvantage	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Social disadvantage	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Causes distress to an individual	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.

May affect an individual's health, well-being or peace of mind	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.

Pension & Investment Product Research

Purpose of Process	To research the market for suitable products which match a clients needs and attitude to risk.
Process Description	Information provided by the client from the fact find is used to research the market for suitable financial products.

Data Subject	Data Category	Data Type
Customers / Clients	Personal data (non sensitive)	Name Address Attitude to risk Pension details Investment details

Legal Basis for processing each category of data

Personal data (non sensitive)	The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Data Update Methods

UpdateMethod:	We rely on the data subject to inform us of changes. We periodically check with the data subject the accuracy of the personal data we hold.

Source of the Data

The Data Subject	

Categories of Data Recipient

Data Recipients:	Restricted staff

Data Retention and Disposal

Retention Time:	Indefinitely
Disposal:	FCA record keeping requirements

Protection Measures

Measures	Pseudo-Anonymisation is used where possible. Backups are automated. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Disable USB & CD Drives to prevent data harvesting or introduction of a virus. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a strong password protection policy. There is a suitably configured firewall in place. Secure connections are implemented. System blocking of certain websites. Email encryption is deployed. Software patches and updates are applied in a timely manner. Timeout screen locks implemented. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. The firm undergoes data protection audits. Due diligence is carried out on third parties. The ICO website is regularly accessed or the firm subscribes to the ICO newsletter. Staff have appropriate background checks. There is a contact point for data subjects. A data protection officer has been appointed. The data protection officer is involved properly and in a timely manner in all issues which relate to data protection. Personal data breaches are reported to the Data protection officer. When engaging the services of another party to process data, an appropriate written contract protecting the rights and freedoms of data subjects is always put in place before any data are transferred. When jointly processing data with another controller, the responsibilities and the essence of any contract are clear and made available to data subjects. Subject access requests procedure implemented. Data protection impact assessments are carried out. Risk management procees is in place. A Business Continuity Plan is in place. Data sharing is appropriate. Our website complies with cookie rules. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. Data search facilities are available. Network monitor software installed. Email filtering of attachments. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.

Data Storage	
Storage	Local hard drive. Local server. Hosted servers. Disk backups.

Pension & Investment Product Research: Risks & mitigating protection measures	
Identity theft	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Staff have appropriate background checks. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Financial loss	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Staff have appropriate background checks. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.

Fraud	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Staff have appropriate background checks. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Damage to reputation	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Loss of confidentiality of data protected by professional secrecy	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Disable USB & CD Drives to prevent data harvesting or introduction of a virus. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a strong password protection policy. There is a suitably configured firewall in place. Email encryption is deployed. Software patches and updates are applied in a timely manner. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.

Loss of control of their data	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Disable USB & CD Drives to prevent data harvesting or introduction of a virus. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Software patches and updates are applied in a timely manner. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Subject access requests procedure implemented. Data protection impact assessments are carried out. Risk management procees is in place. A Business Continuity Plan is in place. Data sharing is appropriate. Our website complies with cookie rules. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. Data search facilities are available. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.
Causes distress to an individual	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.

May affect an individual's health, well-being or peace of mind	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.

Product Application Processing

Purpose of Process	To prepare and submit an application on behalf of a client to a product provider.
Process Description	Client information is prepared and sent to a product provider to assist the client in the purchase of a financial product such as an investment, a pension or some life insurance. Information may be sent by Royal Mail special delivery or via a secure online submission portal made available by the product provider. Product providers act as data controllers in their own right and issue clients with their own privacy notice. The client will know which product provider will be receiving their personal data as this is communicated by the application form or their adviser.

Data Subject	Data Category	Data Type
Customers / Clients	Personal data (non sensitive) Personal data concerning health	Name Address Telephone Numbers Email address Birth certificate Driving licence P45/60 Council Tax information Marriage certificate Passport Nationality Utility bill National Insurance details Bank / building society details Pension details Life insurance details Investment details Employment details Mortgage details Information about a partner Information about dependents Assets and property information Tax information Benefits information Information about marital status Information about age (eg date of birth) Information about gender Information about physical characteristics such a weight and height Other financial details / transactions BMI Details about conditions or illnesses Disability

Legal Basis for processing each category of data

Personal data (non sensitive)	The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
Personal data concerning health	The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

Data Update Methods

UpdateMethod:	We rely on the data subject to inform us of changes. We periodically check with the data subject the accuracy of the personal data we hold.

Source of the Data

The Data Subject	

Categories of Data Recipient

Data Recipients:	Restricted staff, Another controller legally allowed to request and receive information

Data Retention and Disposal

Retention Time:	Indefinitely
Disposal:	FCA record keeping requirements

Protection Measures	
Measures	Pseudo-Anonymisation is used where possible. Backups are automated. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Disable USB & CD Drives to prevent data harvesting or introduction of a virus. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a strong password protection policy. There is a suitably configured firewall in place. Secure connections are implemented. System blocking of certain websites. Email encryption is deployed. Software patches and updates are applied in a timely manner. Timeout screen locks implemented. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. The firm undergoes data protection audits. Due diligence is carried out on third parties. The ICO website is regularly accessed or the firm subscribes to the ICO newsletter. Staff have appropriate background checks. There is a contact point for data subjects. A data protection officer has been appointed. The data protection officer is involved properly and in a timely manner in all issues which relate to data protection. Personal data breaches are reported to the Data protection officer. When engaging the services of another party to process data, an appropriate written contract protecting the rights and freedoms of data subjects is always put in place before any data are transferred. When jointly processing data with another controller, the responsibilities and the essence of any contract are clear and made available to data subjects. Subject access requests procedure implemented. Data protection impact assessments are carried out. Risk management procees is in place. A Business Continuity Plan is in place. Data sharing is appropriate. Our website complies with cookie rules. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. Data search facilities are available. Network monitor software installed. Email filtering of attachments. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.

Data Storage	
Storage	Local hard drive. Local server. Hosted servers. Disk backups.

Product Application Processing: Risks & mitigating protection measures	
Identity theft	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Staff have appropriate background checks. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.

Financial loss	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Staff have appropriate background checks. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Discrimination or unfair treatment	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Fraud	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Staff have appropriate background checks. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.

Damage to reputation	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Loss of confidentiality of data protected by professional secrecy	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Disable USB & CD Drives to prevent data harvesting or introduction of a virus. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a strong password protection policy. There is a suitably configured firewall in place. Email encryption is deployed. Software patches and updates are applied in a timely manner. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.

Loss of control of their data	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Disable USB & CD Drives to prevent data harvesting or introduction of a virus. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Software patches and updates are applied in a timely manner. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Subject access requests procedure implemented. Data protection impact assessments are carried out. Risk management procees is in place. A Business Continuity Plan is in place. Data sharing is appropriate. Our website complies with cookie rules. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. Data search facilities are available. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.
Limitation of their rights	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a strong password protection policy. There is a suitably configured firewall in place. Email encryption is deployed. Software patches and updates are applied in a timely manner. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Subject access requests procedure implemented. Data protection impact assessments are carried out. Risk management procees is in place. A Business Continuity Plan is in place. Data sharing is appropriate. Our website complies with cookie rules. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. Data search facilities are available.

Economic disadvantage	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Social disadvantage	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Causes distress to an individual	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.

May affect an individual's health, well-being or peace of mind	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.

Submission of Business Transactions to Regulated Principal

Purpose of Process	The firm submits business transactions to out regulated Principal to enable them to check compliance and process payment of adviser charges and/or commission.
Process Description	Transactional sale information is provided to or regulated Principal electronically and by providing paper copy information.

Data Subject	Data Category	Data Type
Customers / Clients	Personal data (non sensitive)	Name Address Telephone Numbers Email address Passport Utility bill Attitude to risk Bank / building society details Pension details Life insurance details Investment details Employment details Mortgage details Assets and property information Information about age (eg date of birth) Information about gender Other financial details / transactions

Legal Basis for processing each category of data

Personal data (non sensitive)	The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Data Update Methods

UpdateMethod:	We rely on the data subject to inform us of changes. We periodically check with the data subject the accuracy of the personal data we hold.

Source of the Data

The Data Subject	

Categories of Data Recipient

Data Recipients:	Restricted staff, Another controller legally allowed to request and receive information

Data Retention and Disposal

Retention Time:	Indefinitely
Disposal:	FCA record keeping requirements

Protection Measures

Measures	Pseudo-Anonymisation is used where possible. Backups are automated. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Disable USB & CD Drives to prevent data harvesting or introduction of a virus. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a strong password protection policy. There is a suitably configured firewall in place. Secure connections are implemented. System blocking of certain websites. Email encryption is deployed. Software patches and updates are applied in a timely manner. Timeout screen locks implemented. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. The firm undergoes data protection audits. Due diligence is carried out on third parties. The ICO website is regularly accessed or the firm subscribes to the ICO newsletter. Staff have appropriate background checks. There is a contact point for data subjects. A data protection officer has been appointed. The data protection officer is involved properly and in a timely manner in all issues which relate to data protection. Personal data breaches are reported to the Data protection officer. When engaging the services of another party to process data, an appropriate written contract protecting the rights and freedoms of data subjects is always put in place before any data are transferred. When jointly processing data with another controller, the responsibilities and the essence of any contract are clear and made available to data subjects. Subject access requests procedure implemented. Data protection impact assessments are carried out. Risk management procees is in place. A Business Continuity Plan is in place. Data sharing is appropriate. Our website complies with cookie rules. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. Data search facilities are available. Network monitor software installed. Email filtering of attachments. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.
Data Storage	
Storage	Local hard drive. Local server. Hosted servers. Disk backups.

Submission of Business Transactions to Regulated Principal: Risks & mitigating protection measures

Identity theft	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Staff have appropriate background checks. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.

Financial loss	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Staff have appropriate background checks. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Discrimination or unfair treatment	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Fraud	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Staff have appropriate background checks. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.

Damage to reputation	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Loss of confidentiality of data protected by professional secrecy	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Disable USB & CD Drives to prevent data harvesting or introduction of a virus. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a strong password protection policy. There is a suitably configured firewall in place. Email encryption is deployed. Software patches and updates are applied in a timely manner. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.

Loss of control of their data	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Disable USB & CD Drives to prevent data harvesting or introduction of a virus. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Software patches and updates are applied in a timely manner. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Subject access requests procedure implemented. Data protection impact assessments are carried out. Risk management procees is in place. A Business Continuity Plan is in place. Data sharing is appropriate. Our website complies with cookie rules. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. Data search facilities are available. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.
Limitation of their rights	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a strong password protection policy. There is a suitably configured firewall in place. Email encryption is deployed. Software patches and updates are applied in a timely manner. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Subject access requests procedure implemented. Data protection impact assessments are carried out. Risk management procees is in place. A Business Continuity Plan is in place. Data sharing is appropriate. Our website complies with cookie rules. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. Data search facilities are available.

Economic disadvantage	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Social disadvantage	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Causes distress to an individual	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.

May affect an individual's health, well-being or peace of mind	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.

Protection Annuity Quotation

Purpose of Process	To research the market for suitable products which match a clients needs and attitude to risk.
Process Description	Information provided by the client from the fact find is used to research the market for suitable products.

Data Subject	Data Category	Data Type
Customers / Clients	Personal data (non sensitive) Personal data concerning health	Name Address Attitude to risk Life insurance details Information about interests and pursuits / lifestyle BMI Details about conditions or illnesses Disability

Legal Basis for processing each category of data

Personal data (non sensitive)	The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
Personal data concerning health	The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

Data Update Methods

UpdateMethod:	We rely on the data subject to inform us of changes. We periodically check with the data subject the accuracy of the personal data we hold.

Source of the Data

The Data Subject	

Categories of Data Recipient

Data Recipients:	Restricted staff

Data Retention and Disposal

Retention Time:	Indefinitely
Disposal:	FCA record keeping requirements

Protection Measures

Measures	Pseudo-Anonymisation is used where possible. Backups are automated. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Disable USB & CD Drives to prevent data harvesting or introduction of a virus. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a strong password protection policy. There is a suitably configured firewall in place. Secure connections are implemented. System blocking of certain websites. Email encryption is deployed. Software patches and updates are applied in a timely manner. Timeout screen locks implemented. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. The firm undergoes data protection audits. Due diligence is carried out on third parties. The ICO website is regularly accessed or the firm subscribes to the ICO newsletter. Staff have appropriate background checks. There is a contact point for data subjects. A data protection officer has been appointed. The data protection officer is involved properly and in a timely manner in all issues which relate to data protection. Personal data breaches are reported to the Data protection officer. When engaging the services of another party to process data, an appropriate written contract protecting the rights and freedoms of data subjects is always put in place before any data are transferred. When jointly processing data with another controller, the responsibilities and the essence of any contract are clear and made available to data subjects. Subject access requests procedure implemented. Data protection impact assessments are carried out. Risk management procees is in place. A Business Continuity Plan is in place. Data sharing is appropriate. Our website complies with cookie rules. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. Data search facilities are available. Network monitor software installed. Email filtering of attachments. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.
Data Storage	
Storage	Local hard drive. Local server. Hosted servers. Disk backups.

Protection Annuity Quotation: Risks & mitigating protection measures

Identity theft	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Staff have appropriate background checks. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.

Financial loss	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Staff have appropriate background checks. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Discrimination or unfair treatment	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Fraud	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Staff have appropriate background checks. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.

Damage to reputation	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Loss of confidentiality of data protected by professional secrecy	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Disable USB & CD Drives to prevent data harvesting or introduction of a virus. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a strong password protection policy. There is a suitably configured firewall in place. Email encryption is deployed. Software patches and updates are applied in a timely manner. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.

Loss of control of their data	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Disable USB & CD Drives to prevent data harvesting or introduction of a virus. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Software patches and updates are applied in a timely manner. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Sensitive personal data or large amouts of personal data are only sent using Royal Mail special delivery. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Subject access requests procedure implemented. Data protection impact assessments are carried out. Risk management procees is in place. A Business Continuity Plan is in place. Data sharing is appropriate. Our website complies with cookie rules. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. Data search facilities are available. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.
Limitation of their rights	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a strong password protection policy. There is a suitably configured firewall in place. Email encryption is deployed. Software patches and updates are applied in a timely manner. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Subject access requests procedure implemented. Data protection impact assessments are carried out. Risk management procees is in place. A Business Continuity Plan is in place. Data sharing is appropriate. Our website complies with cookie rules. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. Data search facilities are available.

Social disadvantage	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.
Causes distress to an individual	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.
May affect an individual's health, well-being or peace of mind	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's. TPS/CTPS is consulted prior to marketing calls. Marketing lists only target individuals expecting contact from the firm.

Economic disadvantage	Pseudo-Anonymisation is used where possible. Paper based files are handled securely. Paper files are shredded when no longer needed. Backups are encrypted before transferring to third party servers. Data is accurate and kept up to date. Data is destroyed when it is no longer required. Encryption is used on portable devices. Securely remove all personal information before disposing of old computers. Data protection is implemented by design and default. Consideration to data protection is given before new processes are implemented or personal data are collected. Equipment holding personal data is secured. There is a suitably configured firewall in place. Email encryption is deployed. Role-based access controls implement least privilidge. Origo Unipass has been implemented. Managers control system access. Appropriate policies have been adopted. High risk processes are documented. Staff are trained in data protection requirments. Due diligence is carried out on third parties. Data protection impact assessments are carried out. Risk management procees is in place. Data sharing is appropriate. Portable devices are kept locked away out of sight. An appropriate cloud based service is used to store backups. Antivirus and Malware protection are present on all PC's.