

d3-di-pi-ar | **GDPR** | *legislation.*

25th May 2018 | *General-Data-Protection-Regulation*

The GDPR was approved and adopted by the EU Parliament in April 2016. The regulation will take effect after a two-year transition period and, unlike a Directive it does not require any enabling legislation to be passed by government; meaning it will be in force from May 2018.

The GDPR not only applies to organisations located within the EU but it will also apply to organisations located outside of the EU that offer goods or services to, or monitor the behaviour of, EU data subjects. It applies to companies processing and holding the personal data of data subjects residing in the EU, regardless of the company's location.



GDPR & Parmenion

Your questions answered

Parmenion
It's your future.

Contents

1.	How have Parmenion prepared for GDPR	3
2.	How do Parmenion process personal data?	4
3.	How do Parmenion manage breaches?	5
4.	People and policies	6
5.	Security of personal data	7
6.	Resources	9

1. How have Parmenion prepared for GDPR?

With GDPR coming into effect on the 25th May 2018, we understand that you will be making preparations of your own. To help you with your due diligence on Parmenion, we have created this guide, which aims to answer the most frequently asked questions about Parmenion and our data protection policies and processes.

Nothing has changed in the way we do business, but we have made a number of enhancements to our policies and processes in alignment with GDPR.

Key enhancements include:

Greater transparency - Ensuring updated privacy policies and fair processing notices are visible and accessible to individuals. Creation of records of our processing activities across the business with the applicable lawful processing conditions. Updates to our internal policies, such as our retention policy and standards for ongoing data protection compliance.

We have updated our [Privacy Policy](#) and [Cookie Policy](#). These changes come into effect on 25th May 2018. The updates focus on areas covered by changes in legislation because of [General Data Protection Regulation \(GDPR\)](#) and enhance our existing data protection controls.

Privacy by design - We have provided companywide training to all staff on GDPR obligations, as well as specialised training for staff in specific roles. Incorporation of data protection impact assessments (DPIAs) in relevant areas of project and product design to take account of data protection risks, as well as enhanced due diligence and procurement measures for third party suppliers.

Greater accountability of processing activities - Assessment of our technical and security measures to protect personal data we process. Training and awareness to ensure data breaches are escalated, assessed and triaged appropriately in line with new GDPR timescales. Measures to notify regulator and data subjects as necessary.

More control for individuals over their data - Ensuring we have processes in place to adhere to new subjects rights under GDPR.

2. How do Parmenion process personal data?

What type data does Parmenion process and how is it stored?

Parmenion gather data for different types of data subjects; broadly speaking these fall into three main categories: investors, Advisers and employees. Parmenion's internal processes do not capture sensitive personal data from Advisers or investors as standard practice.

Data processed by Parmenion is mainly stored electronically, though where necessary, we do also store physical records, such as original investment application forms.

Parmenion use various systems to process personal data, ranging from systems we have built in-house to third party software.

Why does Parmenion hold personal data?

Parmenion hold personal data for data subjects for a range of processing purposes. For the vast majority of our processing activities, we hold personal data in order to provide a service; be it the investment services we provide to clients, or the business services we provide to Adviser firms and staff. As an FCA regulated firm, it is also common for us to process personal data to fulfil our regulatory and legal obligations, such as reporting to the FCA and HMRC, or performing necessary legal or regulatory checks.

A common misconception with data protection is that consent is required for all processing of personal data. Whilst consent is one of the lawful processing conditions, there are others that can be relied upon to lawfully

process data. As stated above, Parmenion typically processes personal data in order to provide, or in connection to, a service and would not process personal data in a way that the individual in question would not expect.

Where does Parmenion store data?

Parmenion process personal data in the United Kingdom and European Economic Area (EEA). We do utilise certain providers and suppliers who are located outside of the EEA, however, where we share personal data with such companies, we mandate that all data is processed on servers located within the EEA.

Do you pass data onto any third parties?

Like most large businesses, Parmenion works with third parties who provide products and services that can in turn assist us in enhancing our services to our clients and customers. We may share or utilise a service involving the provision of personal data where necessary, depending on the purpose of processing.

Any third parties that Parmenion outsource to are covered by legal agreements to cover necessary data protection obligations.

Where your staff have access to personal data of our clients and/or employees, is there a confidentiality clause in their employment contracts?

All staff are subject to privacy and confidentiality undertakings as part of employment contract.

3. How do Parmenion manage breaches?

One of the main talking points from GDPR is requirement to report material breaches to the ICO within 72 hours of identification.

Parmenion have existing breach identification and escalation procedures throughout the business. In the event of a data breach, such matters are escalated to the internal data protection function. As with all potential breaches, whether involving personal data or not, necessary action is taken to ascertain the materiality, and further action is taken accordingly.

After a data breach, are your policies and procedures reviewed?

In the event of any data breach, this would be reviewed internally and root cause analysis undertaken to understand how the breach occurred. Following this, we would aim to put controls and monitoring mechanisms in place to prevent or mitigate the risk of a similar incident in future.

Any material breaches would also be reported upwards to our parent company, Aberdeen Standard Investments (ASI), who would support us in the management of the breach.

What is the process by which you would inform the data subject of a breach?

In the event of a serious breach, we would notify affected data subjects and their Advisers accordingly via the most relevant method of communication, along with our regulators.

4. People and Policies

Is Parmenion a registered data controller?

Yes, Parmenion Capital Partners LLP is a registered data controller with the ICO.

Who is responsible for meeting the GDPR requirements?

We have an internal data protection function, supported by our group ownership in Aberdeen Standard Investments (ASI).

Who is your data protection officer?

Parmenion have an in-house data protection function. Should you wish to contact us directly about any data protection queries please contact clientservices@parmenion.co.uk in the first instance.

Do you have a Data Protection policy?

Yes, it can be located on our website under the “Legal” section [here](#).

Do you have a Data Retention and Destruction of Media policy?

We are currently refreshing our retention policy and standards ready for GDPR. Data is held for as long as necessary in line with legal, regulatory or business timescales related to the purpose for processing the data. Once this retention period has ended, and there is no further requirement to process the data in question, we will securely delete / destroy the data via the most appropriate method.

How often is your Data Protection Policy reviewed?

Our data protection policy is reviewed on an annual basis to ensure it remains accurate and up to date.

Who is responsible for the circulation, maintenance and development of your Data Protection Policy?

Parmenion have an in-house data protection function that is responsible for the circulation and drafting of our data protection policy.

Can you fulfil a Subject Access Request (SAR) and right to be forgotten (RTBF) requests?

Parmenion has processes in place to fulfil all data protection subject rights, such as subject access, rectification, and deletion requests. Our [website](#) and [Privacy policy](#) have been updated to include enhanced information about data subject rights as required under GDPR, as well as details of how to exercise these rights.

How is data permanently deleted once it is no longer required in order for you to fulfil your obligations?

Parmenion have the capability to delete data in line with data protection requirements, where necessary, whether the data is in electronic or physical format. The precise method of deletion will depend on the format of the data in question and how this can be effectively put beyond use.

5. Security of personal data

Do you offer regular data protection training to all your staff?

Data protection training is provided to all staff on at least an annual basis. A record of all completed training is kept for each member of staff to ensure knowledge is up to date.

Do you offer additional data protection training to any of your staff (i.e. those working with any sensitive personal data)?

Further in depth specialist training (in additional to the training detailed above) is being provided as part of GDPR preparations.

Parmenion needs to collect and store personal information about Advisers and clients in order to carry out our business. Data is held for as long as necessary to comply with our regulatory obligations and service commitments. Appropriate safeguards are in place to protect all personal data. The platform is located in a secure data centre with restricted smartcard access. Access to our offices is by appointment only and restricted by manned receptions and keycard barrier and doors. The platform data is protected by front and back end firewalls as well as internal firewalls. Automatic intrusion detection alerts are configured to protect our website and databases.

Website security

The website connection is protected by 256-bit AES encryption. This is considered to be very secure and provides a very high level of protection for the personal data that is stored by the website.

Third party data

Where Parmenion enters into contracts with third parties, which may involve access to data, all third party contracts have relevant clauses specifying data confidentiality, and specifically, that all data may only be used in the proper performance of the services being offered.

Data protection

Many aspects of information security are covered in the staff induction process; others are enforced across all staff via our network security.

All employees are subject to background checks as a condition of employment as well as reviewing and signing a code of conduct and compliance undertaking. Regular briefing notes and training are provided to staff to ensure they are aware of their data security obligations.

Group policy is used for a number of security measures such as password complexity requirements, update requirements, automatic workstation locking and remote access together with enforcing file and network security.

Stress testing

The objective of this process is to determine if the website has the capacity to cope with the current website demands and to predict what the maximum capability of the website is before hardware or software upgrades are required.

These results are based on analysis of current usage of the website by existing, registered Advisers. The figures used for the calculations represent peak usage and an additional safety factor of two has been used to allow for unusual usage. These limits are based on the website as it is currently, without any modifications or changes to the hosting.

Based on current capacity, the website can support volumes of ten times the current number of existing users. Stress testing of the website is scheduled to be repeated every six months in order to provide sufficient notice to implement improvements should the need arise.

There are many routes to improve these figures by altering the software and purchasing server hardware. Within reasonable bounds (of work and expense) these figures can be increased by potentially up to a factor of 20.

6. Resources

[ICO Guide to General Data Protection Regulation \(GDPR\)](#)

[ICO: Data Protection Self-Assessment](#)

[ICO: GDPR: 12 Steps to take now](#)

[Article: Consent: option not an obligation](#)

[Article: What does GDPR mean for Advisers](#)



Making investing simpler with Aberdeen Asset Management

Head Office: 2 College Square
Anchor Road, Bristol BS1 5UE.

Office: 0345 519 0100
Website: www.parmenion.co.uk
Email: mail@parmenion.co.uk

Parmenion Capital Partners LLP
Authorised and regulated by the
Financial Conduct Authority.
FCA Number 462085.

Registered in England and Wales
00322243. Wholly owned subsidiary of
Aberdeen Asset Management PLC and
Aberdeen Investments Limited.