



European Union - General Data Protection Regulation
External Frequently Asked Questions

European Union – General Data Protection Regulation – 25th May 2018

European Union – General Data Protection Regulation – 25th May 2018 1

1. What is European Union General Data Protection Regulation (EU GDPR)? 3

2. Why was the existing Data Protection legislation updated? 3

3. What is EU GDPR designed for? 3

4. Where there are conflicts between regulations from other countries, which takes precedence? 4

5. How will Brexit effect EU GDPR? 4

6. What is meant with the term “data subject”? 4

7. What does personal data mean? 4

8. When did the new data protection legislation come into effect? 5

9. To whom does EU GDPR apply? 5

10. I/We am/are not located in the EU, does this regulation apply? 5

11. Does the type of relationship I/we have with FTI make any difference regarding how EU GDPR is implemented? 5

12. Is there anything I/we need to do? What is changing from my/our perspective as a data subject? 6

13. What are the Individual Rights? 6

14. How can the individual rights be requested? 6

15. I/we don’t deal directly with FTI – where should I/we direct an Individual Rights Request? 7

16. What is the data retention policy? 7

17. How and to whom have these changes to Data Protection legislation been communicated? 8

18. What steps have FTI taken internally to ensure compliance with EU GDPR? 8

19. What data minimization efforts are FTI undertaking? 8

20. How will FTI ensure the accuracy of data is maintained? 9

21. What security measures do FTI have in place around personal data? 9

22. How will FTI handle data received from 3rd Parties? 9

23. Is FTI a Processor or a Controller? 9

24. What are the penalties for non-Compliance with EU GDPR? 10

25. What are FTI’s breach response procedures? 10

External FAQs

26. What client documentation has been updated?	10
27. Have distribution agreements been updated?	10
28. Have declarations and disclaimers been updated?	10
29. Are any changes to existing contracts with FTI vendors/suppliers required?	11
30. Who are the data subjects for whom FTI holds personal data, what type of personal data is stored, why is it stored and how is it processed and shared?	11
31. Do FTI transfer data to sub-contractors?	11
32. Is personal data within FTI transferred outside of the EEA? If so where, why & how is this being handled with regards to EU GDPR?	11
33. Who should I/we contact if I/we require more information?	12

1. What is European Union General Data Protection Regulation (EU GDPR)?

The 'European Union - General Data Protection Regulation' (EU GDPR), is a new set of data privacy regulations which builds upon the original framework, to which organizations must adhere.

The regulation impacts all areas where EU personal data is concerned such as retention, privacy and processing rules.

2. Why was the existing Data Protection legislation updated?

The original data protection directive was put in place in 1995, prior to the rise of social media and other online services. As it was in the form of a directive, the way in which it was adopted varied between countries. The purpose of EU GDPR is to ensure that legislation relating to the protection of personal data is "fit for purpose" in today's connected world and to ensure that everyone is implementing exactly the same set of rules. The end data subject should be the main beneficiary, as the legislation should give them more control and ownership of their data.

3. What is EU GDPR designed for?

EU GDPR is designed to

- Introduce higher quality standards on the handling, processing and storage of personal data
- Stress the concept of 'accountability'. Organizations will need to be able to demonstrate EU GDPR compliance and ensure a strong governance framework is in place. Franklin Templeton Investments (FTI) are also working with their business partners and vendors to ensure they fulfil any obligations around the management and protection of personal data
- Strengthen and unify data protection for individuals within the EU, whilst also addressing the export of personal data outside of the EU
- Ensure individuals are well informed (in advance) of what data will be collected from them and for what purpose. Greater transparency is a core theme of EU GDPR
- Appropriately record consent when and where applicable
- React to any potential data breach and notify the relevant regulatory body within a 72 hour period and ensure that the impacted data subjects are notified without undue delay

4. Where there are conflicts between regulations from other countries, which takes precedence?

Where there are conflicts of law between EU GDPR and regulations of countries outside the EU, these will be evaluated on a case by case basis by the Data Protection Officer (DPO) and relevant Legal Counsel as to which law will take precedence.

5. How will Brexit effect EU GDPR?

EU GDPR applies to all companies based in the EU and those with EU citizens as customers. It has an extraterritorial effect, so non-EU countries are also affected. Even though the UK is planning to leave the EU, the UK will still need to comply with EU GDPR if it wants to continue to offer goods and services within the EU. One reason for this is the cross-over period between the UK exiting the EU. The UK will need to comply with the Regulation while it is still a part of the EU. Another reason is the extraterritorial reach of EU GDPR. UK companies continuing to do business with the EU after Brexit will need to comply with the Regulation to avoid infringements.

6. What is meant with the term “data subject”?

The term ‘data subject’ under EU GDPR is a general term which describes any type of individual (identifiable natural person) for whom personal data is stored. For example an active or former investor, prospect, employee, contractor, an independent financial advisor or a related party such as a beneficiary, an authorized signatory, a guardian, etc.

7. What does personal data mean?

EU GDPR applies to Personal data that can be used to identify a natural person.

Personal data means any information relating to an identified or identifiable natural person (‘data subject’).

An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. For example, personal data could be an address, DNA, Facebook profile name, a person’s photograph or any other pieces of information that could, individually or together, be used to specifically identify someone and only that person.

There are also special categories of personal data such as religious belief, sexual orientation, race, ethnic origin, political opinion, health and trade union membership that trigger further data protection requirements.

A natural person means a living person – EU GDPR does NOT apply to legal entities, such as companies or charities, nor does it apply to deceased persons.

8. When did the new data protection legislation come into effect?

The regulation enforcement date is 25th May 2018 based on the law supplied on 27th April 2016.

9. To whom does EU GDPR apply?

EU GDPR applies to any data subject who is located within the 28 EU countries or any other country where Member State law applies. These are the countries of the European Economic Area (EEA) which are Iceland, Norway, and Liechtenstein.

Even where the data of the individual located within the EU is processed OUTSIDE the EU, the legislation will likely still be relevant, depending on the activities undertaken – for example, a company based in the US offering goods and services to German customers will still need to ensure that it complies with EU GDPR.

Equally, where a company located in the EU controlling personal information belonging to an individual outside the EU, they should still comply with EU GDPR.

10. I/We am/are not located in the EU, does this regulation apply?

Under certain circumstances – yes. If the personal data is administered within the EU (for example by a fund domiciled in Luxembourg) this activity will be in scope, regardless of where the personal data originates or the data subject resides.

These rules are extended to those who are in the EU only for a short time (e.g. a holiday) and as well to those from the EU travelling outside.

Note that, nationality is not a factor when determining if a data subject is in scope. Scope focuses on where personal data is being processed and who the personal data refers to.

11. Does the type of relationship I/we have with FTI make any difference regarding how EU GDPR is implemented?

EU GDPR applies to all living individuals, regardless of the nature of your relationship with the company holding your information. Therefore, from an FTI perspective, whether you are an investor, an intermediary, a dealer/broker or have any other form of relationship with us, we will apply EU GDPR with respect to your personal data. However, please be aware that **how** we can apply EU GDPR may vary, dependent on the nature of your relationship and other applicable laws, such as anti-money laundering legislation and other financial regulations.

12. Is there anything I/we need to do? What is changing from my/our perspective as a data subject?

As a data subject, it is recommended to review the applicable Privacy Notice for full details on how we use, retain and treat your data. Our relationship is not changing, we are simply clarifying your rights and our responsibilities with respect to information we hold about you as an investor, business partner, distributor etc.

Please see our updated [Privacy & Cookie Notice](#)

13. What are the Individual Rights?

EU GDPR introduces new rights for Individuals and enforces existing expectations relating to:

- The right to be informed
- The right to access personal data
- The right to rectification of incorrect details
- The right of erasure –FTI cannot keep data for longer than it is required for the purpose for which it is collected
- The right to be forgotten - Individuals can request to have their personal data removed under certain circumstances
- The right to object to certain data processing activities (e.g. profiling)
- The right to the restriction of processing
- The right to data portability

14. How can the individual rights be requested?

If an individual wishes to make an Individual Rights Request, they must contact FTI in writing by post, fax or email providing all information which is requested in our request form. Therefore, it is preferred that they submit a request to FTI by completing a Rights' Request Form however, legally they are within their right to submit via other means.

Please refer to our [Privacy & Cookie Notice](#) where the Rights Request Form can be obtained.

The Request forms and the email submissions should be submitted to DataProtectionOfficer@franklintempleton.com

The Address for post submission:
Franklin Templeton International Services S.à.r.l.
FAO: Data Protection Officer
8A, rue Albert Borschette
L-1246 Luxembourg,
Grand Duchy of Luxembourg.

The Fax Number for submission +352 46 66 76

Upon receipt the request will be verified, considered and a decision made regarding whether FTI are in a position to complete the request, need further information or are unable to fulfil the request for any reason. In line with the legislation, FTI will communicate back to the individual whether FTI have completed the request or are unable to complete the request within 30 days of receiving a fully completed Rights Request Form/written submission with adequate details included. All requests, their subsequent decision, execution and all communications with the data subject will be recorded and documented and may be provided to the Supervisory Authority if requested.

15. I/we don't deal directly with FTI – where should I/we direct an Individual Rights Request?

All our clients serviced by 3rd Parties can either submit a request directly to us (see Q13) or via our 3rd Parties by submitting the FTI Rights Request Form by post, email or fax to them. Each request will be reviewed on a case by case basis.

16. What is the data retention policy?

FTI will retain personal information covered by the updated Privacy Policies for as long as required to perform the purposes for which the data was collected, depending on the legal basis on which that data was obtained and/or whether additional legal/regulatory obligations mandate that FTI retain the personal information.

In general terms, this will mean that personal information will be kept for the duration of the relationship and for the period required by tax, company and financial service laws and regulations. It may differ from jurisdiction to jurisdiction however, in the majority of cases, this will be during the relationship and then for 7 or 10 years after the end of the relationship, depending on the type of information held.

17. How and to whom have these changes to Data Protection legislation been communicated?

As part of FTI's EU GDPR Global initiative, this change has been communicated along with links to FTI's updated Privacy Notice documents to our existing shareholders and their related parties.

Furthermore, all in scope contacts of the Sales and Marketing teams within FTI received a communication about this change.

Other affected parties such as institutional investors, 3rd party TAs and platforms, distributors, vendors, external law firms and board members have also received communications outlining the changes.

18. What steps have FTI taken internally to ensure compliance with EU GDPR?

In early 2017 FTI initiated a Global Program in order to implement the necessary changes and ensure a robust plan was in place to address the agreed areas of compliance by the effective date. The Program covered all impacted business areas across the globe.

FTI addressed the key areas of change as follows:

- Business processes and system level functionality to support individual Rights Requests updated
- Evaluated a corporate solution to centralise and track individual Rights Requests
- Partnered with Legal and Compliance to document a DPO (Data Protection Officer) Framework
- Expanded the existing Data Protection policy to meet EU GDPR compliance
- Vendor liaison where development activities were required to support individual rights

Business Unit Readiness (BUR) was also addressed. Here are some of the main focus areas:

- Client Documentation updated
- External communications completed
- Privacy notices created and distributed
- Contract reviews and required updates with FTI's business partners and vendors completed

As required by the regulation, an experienced EU Data Protection Officer (DPO) has also been appointed by the Franklin Group. He is based in Luxembourg and oversees all aspects of EU GDPR.

19. What data minimization efforts are FTI undertaking?

FTI have continued to minimize data where applicable. As part of EU GDPR, FTI have completed a review exercise to ensure are compliant with the new more strict requirements. As part of this exercise, it was determined that all data held within FTI had a “legitimate purpose”. FTI continually review and look to remove any data duplication where possible within organisational and regulatory frameworks.

20. How will FTI ensure the accuracy of data is maintained?

FTI has always taken great care to ensure data is accurate and prior to EU GDPR, had in place many controls and procedures to ensure that data was correct. Further to EU GDPR, no additional actions have been identified as being necessary to ensure the accuracy of FTI data.

If you have identified any data FTI hold about you which you believe to be inaccurate, please get in touch via existing methods in order to have this amended by our usual business procedures such as a Data Change Order. Should it not be updated correctly or in a timely manner, you can complete a “Right to Rectification” Individual Rights Request Form.

21. What security measures do FTI have in place around personal data?

FTI have a series of information security controls in place to protect the confidentiality, integrity and availability of shareholder and business information from anticipated threats. There are also technical and organizational controls which protect the rights and freedoms of the data subject (with specific reference to transparency, access to personal data, information from where the personal data was collected, right to rectification, right to erasure, right to restrict processing, right to data portability, and right to object). The policy also ensures FTI must implement the appropriate security measures to safeguard Confidential Information specified in applicable laws and regulations.

22. How will FTI handle data received from 3rd Parties?

FTI will treat any personal data received via 3rd parties with the same integrity as they would all other data when ensuring security, accuracy and minimisation.

23. Is FTI a Processor or a Controller?

Under EU GDPR, institutions that collect and process personal data are viewed as either as Controllers or Processors of Personal data.

Under article 4 of the Regulation, Controllers and Processors of personal data are defined as follows:

- Controller – “means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data”
- Processor – “means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”

FTI has many Business partners and these relationships are multifaceted to meet the business needs. The different nature of these relationships means to some of our partners FTI are Controller or joint Controllers of data but to others FTI are processors.

24. What are the penalties for non-Compliance with EU GDPR?

Non-compliance for both FTI and external parties could potentially incur a fine of up to €20 million or 4% of global turnover, whichever is greater. This is a dramatic increase from the previous directive.

25. What are FTI’s breach response procedures?

Data security breaches will be managed in line with EU GDPR. The relevant personal data subjects will be informed of any data breaches where legally required.

26. What client documentation has been updated?

FTI have amended all impacted client documentation with appropriate EU GDPR updates, including Application Forms and Prospectuses for the in scope funds.

27. Have distribution agreements been updated?

FTI’s distribution agreement template has been updated with a short paragraph about EU GDPR.

It is not planned to update the majority of the existing agreements since they contain a general obligation for distributors already to act in compliance with ‘all applicable’ laws.

FTI however, has updated the existing agreements with those distributors who are acting as processors, for example our distributors in Italy and Poland.

28. Have declarations and disclaimers been updated?

External email disclaimers have been updated where applicable to include the link to FTI's Privacy & Cookie notice.

29. Are any changes to existing contracts with FTI vendors/suppliers required?

Vendors with whom FTI do business and who are in scope of EU GDPR will be required to enter into industry standard contract addendums with us that will cover all the relevant aspects of EU GDPR to ensure compliance if they are confirmed as processors.

30. Who are the data subjects for whom FTI holds personal data, what type of personal data is stored, why is it stored and how is it processed and shared?

Please refer to the [Privacy & Cookie Notice](#) which can be found here in many different languages.

Personal data is stored for a number of reasons:

- Consent is given by the data subject
- The personal data is necessary to perform a contract
- Regulatory obligations
- Protection of vital interests
- Protection of public interests
- And legitimate interests

31. Do FTI transfer data to sub-contractors?

FTI's Business model does require the use of sub-contractors. FTI will share personal data with relevant sub-contractors in order to fulfil a Business requirement. All agreements and contracts with these sub-contractors have been updated to ensure that the same level of protections and the same rights are in place as with FTI

32. Is personal data within FTI transferred outside of the EEA? If so where, why & how is this being handled with regards to EU GDPR?

Data may be transmitted or accessed between the EU offices and non EU Offices via FTI systems including email and SharePoint.

For more details please refer to the [Privacy & Cookie Notice](#)

33. Who should I/we contact if I/we require more information?

Your first point of contact should be via the existing communication methods you have with us whether that be through your local Client Dealer Service Office or Sales & Marketing Team.

If they are unable to assist, they will liaise with the applicable internal Data Protection Coordinators (DPC) or Data Protection Specialists (DPS) in order to respond to you effectively.

For more complex questions, they may also reach out to the Data Protection Officer (DPO) whom you may also prefer to contact directly using the email address:

DataProtectionOfficer@franklintempleton.com