# General Data Protection Regulation – GDPR

The GDPR will take effect in the UK on **25th May 2018**. The Government have confirmed their decision to leave the EU will not affect the commencement date of the GDPR. The adoption of the GDPR, will lead to the repeal of the Data Protection Act.
As it's important that you comply with the GDPR, especially with increased fines in the offing, we have provided an overview of the requirements so that you can start to prepare your firm.

## What is the current position?

How you collect, store, use and hold personal data of your clients and employees is currently governed under the Data Protection Act 1998 (DPA). Just as Fast Forward Technology Ltd are required, you also are required to be registered data controllers and hold an ICO data protection licence and are responsible for the personal data, both client and employee data, and are required to comply with the 8 data protection principles under the DPA.
To support data controllers with their DPA compliance, Fast Forward Technology Ltd already provides a collection of supporting documentation.

## What is the new regulation?

Whilst the basic principles of the existing regime will be retained, the GDPR will introduce new concepts and new rights for the data subjects some of which will have a significant impact on how you handle and use personal data.
The biggest change is the increased fines for data breaches. Currently under DPA the ICO fines have been limited to £500k, but GDPR **increases this to the higher of 4% of the annual turnover or €20,000,000.**
Currently the FCA and ICO have worked together in relation to a data breach involving a regulated firm with the FCA imposing greater sanctions. However, in the GDPR world, data controllers will need to be prepared for the ICO taking stricter enforcement action independently of the FCA to utilise the increased fines creating an additional financial risk in addition to the existing legal and reputational risk.
On the next page we have included a useful summary of all the changes that GDPR will bring, together with recommendations on actions we recommend you take.

# Summary of GDPR and recommendations

| GDPR requirement | Areas to consider as data controllers | Recommendations to meet GDPR requirements |
|---|---|---|
| **Data Retention:**<br>♣ Personal data to be retained no longer than necessary.<br>♣ Retention periods to be notified to individuals. | Client files need to be retained indefinitely to defend advice liability claims that may arise at some point in the future. This is justified on the basis that the long stop date of 15 years has been removed for consumers bringing complaints in relation to financial services advice. This undefined retention period is contrary to GDPR principles. | 1. Introduce/ revisit retention policy to all documents that include personal data<br>2. Fast Forward Technology Ltd are considering a finite retention period for client files that is justified and defensible;<br>3. Destroy personal data on expiry of retention periods. |
| **Data processing:**<br>♣ Identify legal grounds for processing:<br>o explicit consent;<br>o Performance of a contract<br>o Meeting legal obligations;<br>o In the legitimate interests of the data controller. | The legal grounds for processing personal data for data controllers are:<br>1. Reliance on the performance of a contract i.e. the client agreement; and<br>2. Reliance on the grounds for meeting legal obligations (FCA requirements) and in the legitimate interests (promote or manage the business) of the data controller.<br>Under GDPR the grounds for relying on client consent to process data are more onerous and should be avoided where possible. | 1. Avoid relying on consent to process personal data; instead rely on the other key grounds.<br>2. Document the grounds for data processing activities carried out by your firm;<br>3. Review client agreements and privacy notices to include wording about what processing activities you do with client data and remove consent wording where appropriate. |
| **Privacy notice:**<br>Privacy notice is a statement that provides certain information to individuals about how their data is collected, stored used and must include data retention periods, rights of appeal, rights of data portability and erasure, details of DC and DPO. | Current privacy statements included on the client agreement, websites, and application forms may not include all the required information. | 1. Identify all points at which personal data is captured and where a privacy notice must be provided to individuals (clients, employees);<br>2. Draft a privacy notice applicable for clients and employees and incorporate it into business operations. |
| **Data erasure:**<br>Request from an individual to delete all data. | The right to erasure is not absolute, if the data controller can show a clear regulatory or other legitimate ground to retain the data, they need not comply. Data controllers should retain evidence where data is deleted on request. | 1. Develop clear procedure to:<br>a. identify data;<br>b. articulate the justification for retaining client data beyond the life of a contract in order to explain this position to data subjects or to the Information Commissioner, and<br>c. delete data<br>2. Prepare template responses to client's data erasure request. |
| **Data portability:**<br>To meet the individual's right to receive in machine readable form all the personal data they have provided to the organisation. | Clients' personal data they have provided may be stored in a number of places, e.g Fast Forward Technology Ltd, other back office systems, filing cabinets. This information needs to be located to answer a data portability request. | 1. Map the extent of personal data received from clients and likely to fall within the terms of the data portability right.<br>2. Develop a procedure for efficient retrieval and output of data in response to requests.<br>3. Mandate the use of one system in your firm i.e. (Fast Forward Technology Ltd). |

| | | |
|---|---|---|
| | Data minimisation will help simplify such requests.<br>Storing client personal data and information in one system ie Fast Forward Technology Ltd Advantage will also simplify the process for dealing with portability requests, data erasure requests and DSARs. | |
| **Third party data processors:**<br>Data processors face new liability obligations. | Consider third parties who process data on your behalf e.g. Fast Forward Technology Ltd for providing compliance and support service, 3rd party IT providers, outsourced para planners, marketing agencies. | 1. Identify all data processing activities and review contracts or introduce additional data processing agreements.<br>2. Identify DP activities Fast Forward Technology Ltd carries out on your behalf. |
| **Data breaches:**<br>The statutory obligation to report significant breaches is new in GDPR. | Data controllers are required to report breaches and near misses (incidents) under current policy. | 1. Revisit your incident reporting process.<br>2. Raise the profile of reporting within your organisation.<br>3. Share learning outcomes from breaches and near misses. |
| **Data protection by design / data protection impact assessment:**<br>♣ "Data protection by design" requires a more granular approach which ensures the minimum amount of personal data is captured in the first instance and the data is further minimised as processes permit.<br>♣ DPIA-mandatory for high risk processing | ♣ Collect the minimum amount of personal data for the specific purposes.<br>♣ It is unlikely that Members or clients meet the high risk threshold where DPIA are mandatory, however its good practice to carry out an assessment where a project would involve a significant change to the processing of personal data. | 1. Embed principles of data minimisation and privacy controls into business process design and systems development. Develop a challenge culture where departments keep under review the personal data that they capture and retain.<br>2. Watch out for further guidance on DPIA from ICO. |
| **Data protection officer:**<br>A DPO is mandatory for organisations where there is large scale data processing of special categories of data. | Data controllers should designate someone to take responsibility for data protection compliance and assess where the role sits within their organisation. That person should have expertise to meet the privacy responsibilities of the organisation. | 1. Formalise DPO role and provide appropriate training.<br>2. Outsource DPO requirements to 3rd party if applicable. |
| **Accountability and transparency**<br>Organisations to be responsible and accountable for their GDPR compliance. | Currently under ICO members and select clients are required to register as data controllers. Under GDPR, rather than register with the ICO, you will need to be able to evidence your compliance with the GDPR through systems and processes you have in place. | 1. Data controllers to document the systems and processes it has in place to ensure GDPR compliance that should include a list of all applicable policies, business systems and their owners. |
| **Staff training:**<br>**Staff awareness is critical to protecting personal data.** | On line staff training and assessment are provided to members. Data controllers are required to ensure their staff have DP training. | Review and update training material. |