10 things financial advisers need to know about GDPR

With the General Data Protection Regulation (GDPR) deadline fast approaching, any firm that handles data and/or engages in any form of marketing to consumers needs to prepare itself to comply. Failure to do so could prove catastrophically costly. The central tenet of GDPR is to greater protect the rights of individuals as concerns their data. We take a look at the need to know elements within the regulation that firms need to get started with straight away.

1. When does GDPR kick in?

GDPR is currently in a grandfathering period and you have until 25 May 2018 to be compliant. All activity thereafter which fails to comply to with the regulation could see huge penalties handed out. GDPR will be enforced by the UK's supervisory authority for GDPR, the Information Commissioner's Office (ICO).

2. What are the penalties?

The headline numbers are massive - €20,000,000 or four percent of global revenue, whichever is highest. Of course, no one knows for sure if such fines will be handed out, but it is clear that a very dim view will be adopted by the regulator in the event of a breach of the regulation. There is also an updated right for data subjects to claim compensation for damages they suffer from such incidents. Such law suits would be in addition to any fine levied by the ICO.

3. Brexit will not save you

Some of the feedback that we've had from our clients in response to content we've produced on GDPR has been, "This is an EU regulation and we're leaving, so I don't care." This stance could not be further from reality. The UK government played a major hand in writing the new laws and it will be transposed fully into UK law, even once the UK has made its exit from the EU.

4. How you can end up before the regulator

Scenario 1. A member of the public (the data subject) could report you to the ICO. For example, if you contact individuals who have not consented to being contacted by you, or are not expecting to be contacted by you, they could report you to the ICO.

Scenario 2. You may have to report yourself! GDPR introduces strict rules about notifying the regulator within 72hrs of identifying a breach where the rights and freedoms of your clients are at risk. For example, this could include the loss of an unencrypted laptop or USB stick. It could also include theft of data via a cyber security breach. In both instances, if client data has left your control, you may have to report it to the ICO and also notify your customers.

5. How do I report, and to whom?

Reporting needs to be done within 72 hours of knowing that a breach has occurred. The ICO needs to be notified and, in some cases, the individuals' whose details are concerned, too.

If an unencrypted laptop containing client data has been stolen, then this would constitute a breach and you would be required to explain why it was unencrypted and what the likely consequences of the loss are to the individuals concerned.

In such circumstances, the individuals would also need to be notified where it is likely to result in a risk to their rights and freedoms. This is where they could be subject to identify theft, fraud, financial loss, reputational damage or loss of confidentiality as a result of your actions.

The report to the ICO will need to contain information on the nature of the breach, the number of individuals concerned (approximately), categories lost and details of the likely consequences of the breach. It will also need to be outlined to the ICO how the breach will be dealt with.

Consider how you will report a breach now – it is important to have the correct procedures in place in advance of an event.

6. Accurate data only

Keeping and processing inaccurate data will only lead to trouble. You need to be sure that the individuals being contacted wish to be contacted and that the plan data you hold on them is accurate. If data is muddled, the pitfalls are obvious.

Maintaining accurate data can be tricky, but keeping records up to date with active clients and prospects is essential, as is planning for maintaining the accuracy of such data.

If you have old data, consider whether or not you really need to keep it. If you don't, then delete it. If you do, take steps towards ensuring its accuracy. If you can demonstrate that you have taken reasonable steps towards to ensuring accuracy, then this will be well received by the regulator in the event of any mishaps or complaints against you.

7. Contact legacy clients now

If you wish to continue contacting legacy clients and prospects after 25 May 2018, then you need to gather the evidence that they wish to be contacted by you now. After 25 May, sending out requests for permission to contact people will constitute a breach, since you will not have consent from them to undertake such an activity. If you seek permission and no affirmative action is taken by the individual being contacted, this does not constitute consent under GDPR and you will be unable to contact that individual again.

Of course, with clients and legacy clients, some contact is necessary for the performance of your contract with them, such as portfolio valuations and annual statements. These are necessary touch points. Marketing a new investment opportunity, for example, is not and requires unambiguous consent.

8. Portability, availability and the right to be forgotten

GDPR makes allowances for individuals to take greater control over the processing of their data and this includes moving their data from one provider to another. Upon receipt of such an instruction from a client, you will need to provide their data without undue delay, i.e. within one month. The data should be made available in an easily readable format. This doesn't mean that you need to bring your data processing in line with other firms or an industry standard, just that it can be easily understood by the recipient.

Individuals can also request access to their data to see what you hold on them. Again, this should be done without undue delay, i.e. within one month.

Finally, individuals can request that you forget them, i.e. delete them from your database. For financial advisers, where previously advised clients may have legal recourse on your engagement with them, the request to be forgotten can be refused, but only where you will need the data in future circumstances. Otherwise, the data you hold on them must be deleted.

9. Privacy by design

Simply making colleagues aware of GDPR is a massive step in the right direction. Ultimately, it is the responsibility of everyone. If one of your colleagues accidentally emails a spreadsheet with data on individuals to a wrong email address, for example, this constitutes a breach and an easily avoidable one at that.

So make sure everyone is aware of the regulation and their responsibilities. Privacy by design is what the regulator is looking for and training is an essential step towards achieving that. By having relevant documents and procedures in place, you will also have evidence to provide to the regulator that steps have been taken towards ensuring compliance.

10. Show your workings

The ICO states: "The new accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility."

Much like those maths tests you used to take at school, showing your workings is an important step towards achieving high scores (or avoiding high penalties) under GDPR. The regulator will certainly take a dim view of incidents where there is no evidence to support a case for events occurring beyond your reasonable control.

If, however, you can show that reasonable steps have been taken towards avoiding a breach, or ensuring data accuracy, then it is far more likely that the regulator will adopt a sympathetic stance with you.

Intelliflo is working closely with its clients and the financial advice industry to help with GDPR compliance.

For more information on how we can help you, please visit: **www.intelliflo.com**