The new world of GDPR
Fund managers confronted by tough EU data protection and privacy rules

Andrew Churchill, Digital Innovation Director at TISA
(Tax Incentivised Savings Association)

Few people in the funds industry, let alone among the general public, are aware of the General Data Protection Regulation (GDPR), which comes into effect in May 2018. Fewer still are aware of the concurrent e-Privacy Regulation, though as the latter is still partially in negotiation we shall focus attention on changes in data protection.

The GDPR is potentially a game-changer – firstly, in that it requires organisations to dramatically improve how they gather, use, store and disclose personal data on employees, contractors and customers across the European Union.

A potent piece of legislation

The GDPR represents a major shift from the current privacy regulatory environment in the EU.

You just need to consider the penalties for non-compliance to see how seriously the EU regards this regulation. Fines of up to 4% of global turnover, or €20 million, whichever is higher, can be levied for the worst breaches, which will need to be notified to the relevant regulator within 72 hours. Obviously, this is the part that gets the most column headlines too.

The UK will still be a member of the EU when GDPR comes into force in May 2018, and the Information Commissioner's Office is adamant that they will enforce it from that date, but even on its eventual exit, GDPR is still likely to apply to the UK since the regulation is applicable to any firm which processes the personal data of EU citizens.

It is also important to note that, unlike the current Data Protection Act in the UK, GDPR is a Regulation, and therefore should be harmonised across all 28 Member States. This is a seemingly minor, but fundamental distinction – the existing UK Data Protection Act is the UK national transposition of the EU Data Protection Directive – effectively the UK version, with a potentially different version in other Member States.

Confusion still remains

This has been a cause of confusion for multi-nationals for some time, so GDPR may well help organisations in this regard.

Given that UK fund management companies will certainly seek to continue to offer products and services to EU investors, it is possible that the UK will directly adopt GDPR or, alternatively, create a home-grown rule which closely matches the Regulation, potentially in a similar vein to the US-EU Privacy Shield arrangements that currently enable US firms to handle EU citizens data.

Either way, there will potentially be differences in how the rule is applied in different Member States, including the UK, and uncertainty on how enforcement will be handled in different Member States is an obvious cause for concern for business, particularly if there are different prioritisations given to different facets of data rights from jurisdiction to jurisdiction.

Even within a single country such as the UK, however, it is imperative that businesses understand how the Regulator will enforce the regulation, and it is achieving this transparency that will be crucial, and as far in advance of the May 2018 date as possible.

Alignment

This need for transparency underlines the importance of establishing, in close co-ordination with the Information Commissioners Office (ICO), an industry code of conduct in how financial services firms should handle data.

Fortunately, work has been underway for some time in establishing underlying data sharing principles, with a working group currently finalising its initial report on these principles.

The next step, and the task for the next 6-9 months, however, is to evolve these principles into a practical code of conduct against which organisations can measure their degree of compliance, so as to better understand – and understand in agreement with their regulator – their degree of risk of liability when losses inevitably occur if losses occur.

Whilst many sectors of the economy will need their own specific interpretations of GDPR, the financial services industry has, perhaps, the most exceptions to manage given our simultaneous regulatory requirement to store data – sometimes even against the wishes of the data subject.

This is why TISA and its members are keen to support the ICO in the creation of this vital code of conduct, and we will soon formally launch our working group to take this work forward, building on the existing material we have developed with the data sharing principles working group to take this work forward, building on the existing material we have developed with the Data Sharing Principles working group.

I encourage you to join us in this endeavour and please do contact me for details of our launch event that will shortly be scheduled for later in July.