Cybersecurity and data protection

By Lucy Frew

Significant developments in the regimes for data protection and cybersecurity, together with increasing investor awareness, mean that these are key issues for hedge fund businesses in 2018.

Technological advances have brought great opportunities and efficiencies to the alternative investment fund industry but not without also introducing previously unimagined risks, irrespective of geographical location.

With the introduction of new domestic legislation in the form of the Data Protection Law, 2017 (DPL), new international regulation in the form of the General Data Protection Regulation (GDPR) and heightened regulatory scrutiny from the Cayman Islands Monetary Authority (CIMA), investor demands, as well as commercial and reputational risk sensitivity, mean that data protection and cybersecurity are topping hedge fund businesses priorities lists for 2018.

Lucy Frew, Partner, Walkers (Cayman Islands)

Regulation

Across the world, including the Cayman Islands, governments and regulators have been steadily increasing their focus and resources on cybersecurity. Ironically, it is also the legal and regulatory obligations to collect personal data resulting from new international data sharing regimes combined with cybersecurity concerns and innovative technology deployments which are making the regulation of personal data more complex than ever before.

CIMA had already announced in May 2016 that it sees cyber attacks as one of the key risks facing the financial sector in today's digital environment.

CIMA has strongly encouraged licensees to assess their cybersecurity risks, reassess their strategies to ensure they are comprehensive and up-to-date for the current environment and to test their security programmes to identify vulnerabilities to their systems. CIMA had already made clear it will review licensees' approaches to data security risk management and examine technical controls, incident response, and staff training. As part of its reviews, CIMA will also consider licensees' ability to protect the confidentiality, integrity and availability of sensitive customer and other information.

Financial regulators, including CIMA, are typically not being prescriptive in setting out rules and standards to which alternative investment funds sector businesses must adhere. This makes sense given the breakneck pace of sophistication of both cyber attacks and prevention. However, CIMA is certainly increasing its focus on the issues of cyber risks and cybersecurity within the industry, especially as the industry is playing an ever-increasing role in financing the economy.

General Data Protection Regulation and the Cayman Islands

Commencing 25th May 2018, GDPR will replace the current EU data protection regime. It will apply not only to organisations in the EU but also to organisations based outside the EU if they collect or process personal data of EU individual; for example, in the context of a fund, when collecting anti-money laundering, FATCA or CRS information.

The Cayman Islands is not part of the EU and has not implemented GDPR. Nevertheless, one of the key changes under GDPR is the extension of territorial scope to include data controllers and processors that are not established within the EU but whose data processing activities relate to 'offering goods and services to individuals in the EU' or 'monitoring behaviour taking place in the EU'.

A number of alternative investment fund sector businesses that were not within scope of the predecessor regime will now be captured and will need to ensure that their processes are compliant with GDPR.

In terms of what is meant by "offering", it is important to distinguish the application of GDPR from that of the AIFMD. Offering will only be within scope of GDPR if personal data is actually processed. In other words, if a third country manager hands a non-individually addressed offering document to a prospective investor in the EU, the manager would likely be regarded as marketing under the AIFMD but not necessarily without more, as processing personal data for the purposes of GDPR. However, any related processing of personal data would constitute processing activities related to the offering of goods and services in the EU.

Conversely, activity may constitute processing of personal data for the purposes of GDPR even if there is no marketing within scope of the AIFMD. For example, a manager may collect investor contact details with a view to a future fund offering without, at that point, attempting to communicate with such investors. Nevertheless, such collection of personal data would likely constitute processing of personal data under GDPR.

The other basis which might bring a hedge fund business with no EU establishment and no EU investors into scope relates to "monitoring behaviour taking place in the EU".

A processing activity should be considered monitoring where EU data subjects are "tracked on the internet." This includes the possible subsequent use of the acquired data for the purposes of "profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes". This is relevant where, for example, a manager outside the EU uses alternative data or data analytics based on behavioural monitoring of data subjects in the EU.

Relationships with entity investors, as well as individual investors, are likely to involve the processing of personal data of natural persons. An individual who invests in a fund is usually required to provide a host of personal data. A company, partnership or trust investor in the fund is usually required to provide personal data in relation to its individual directors, members, shareholders and other beneficial owners. It follows that even if all investors are located outside the EU, one cannot rule out the possibility that onboarding will involve personal data of individuals in the EU.

The Data Protection Law, 2017

The DPL will introduce for the first time a data protection regime in the Cayman Islands. The DPL was gazetted on 5th June 2017 and will come into force on a date set by Cabinet Order, expected to be January 2019. Meanwhile, regulations will be made in relation to various provisions of the DPL. As the DPL is based on the UK and EU data protection legislation, its definitions and concepts will look very familiar to UK or EU managers or service providers to Cayman Islands hedge funds.

Similar to its predecessor legislation, GDPR restricts transfers of personal data beyond the EU to ensure it is being sent to a country which provides for adequate data protection. By implementing the DPL, the Cayman Islands are beginning the process towards achieving "equivalence" status. Meanwhile, transfers of personal data can be made in the absence of adequacy decisions in various circumstances including where the individual has consented.

Data protection and cybersecurity

Compliance with GDPR and DPL overlap to a significant degree with hedge fund businesses' cybersecurity measures. Controllers must implement appropriate technical and organisational measures to ensure the protection of personal data during processing and transfer and to prevent unauthorised or unlawful processing of personal data and accidental loss or destruction of, or damage to, personal data.

Sanctions for failure to secure personal data and enforcement

The DPL contains significant financial penalties but these do not compare to the size of those under the GDPR, where businesses that fail to comply with the GDPR's data security requirements may face fines of up to EUR20 million or 4 per cent of total worldwide annual revenue; whichever is greater. The extent to which EU authorities will investigate and take enforcement action against organisations with no EU establishment remains to be seen especially if, as is likely in the case of hedge funds, there is little to no detriment to the retail public. ■