Protecting personal data: is the industry prepared?

The new Cayman Islands Data Protection Bill will regulate the future processing of all personal data in the Cayman Islands. Fund managers should take steps now to ensure that they understand their obligations, say Sailaja Alla and Peter Colegate of Appleby's Cayman Islands office.

Investors in funds increasingly require and demand data privacy. As obligations to collect personal data increase with new international data sharing regimes, fund managers need to pay close attention to data protection issues. These international obligations, together with cybersecurity concerns and innovative technology deployments are making the regulation of personal data more complex than ever before. Fund managers need to get it right—reputations and criminal liability may soon be at stake.

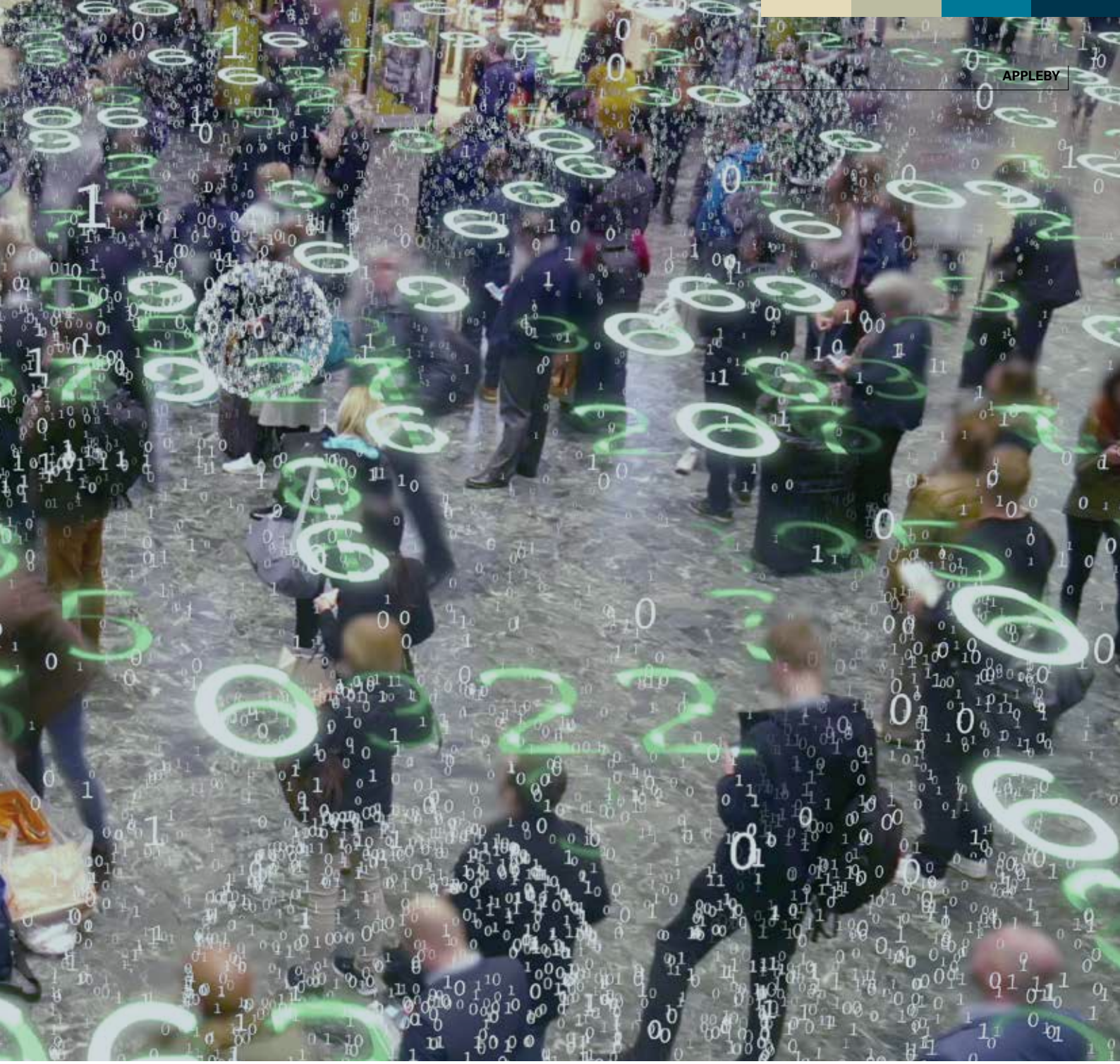
The new Cayman Islands Data Protection Bill, likely to pass in the near future, will regulate the future processing of all personal data in the Cayman Islands. Fund managers should take steps now to ensure that they understand their obligations under the Bill, that they have in place policies and procedures to ensure the proper protection of personal data under their control and that they develop a culture of compliance in relation to the collection and management of personal data that is understood throughout their business.

Impact on the funds industry

Drafted around a set of internationally recognised privacy principles, the Bill provides a framework of rights and duties designed to give individuals' greater control over their personal data. The Bill supports a growing expectation from international businesses and their clients that organisations operating in offshore jurisdictions have in place comprehensive data protection compliance requirements backed up by robust data privacy legislation.

Personal data is defined widely to include any data relating to a living individual. The average fund generates and retains a huge amount of personal data. Fund managers hold proprietary research and investment strategies, proprietary and personal information about markets, companies and individuals, high value email and contact lists and net worth information for individuals.

Under the Bill, the personal data held by the fund must be processed fairly and lawfully and used for a legitimate purpose that has been notified to the data subject in advance. Personal data holdings should not be excessive in relation to the purposes for which they are collected and should be securely purged once those purposes have been fulfilled. If personal data are processed for any new purposes, this processing can only be undertaken if fresh consent is obtained.



While it is very unlikely that a fund manager will use personal data other than for the purposes of processing an investment and meeting legitimate reporting and record-keeping obligations, the fund must set out the purposes for which personal data is being collected and details of whom that data may be shared with. Data subjects must also be informed of any countries or territories outside the Cayman Islands to which their personal data may be transferred.

Recommended best practice would be for this information to be set out in a separate privacy notice which can be provided with the offering memorandum and subscription documents.

Transferring data to third parties

Fund managers' operational, trading and back-office functions are now mostly digitised and delegated to external service providers. In an age where highly sensitive information can be exchanged at the touch of a button, data protection issues must be considered before any transfers of personal data are made to third parties. There is no substitute for proper due diligence on the systems, policies and procedures of those providers to ensure that personal data are handled appropriately and securely. Regular physical audits and independent testing of a service provider's controls would also be advisable.

Contractual provisions should be put in place between the fund (as the data controller) and the third party service provider (as data processor) to ensure that any personal data are processed only for authorised purposes, that all data are stored and transmitted securely and that disaster recovery practices are in place in the event of a data breach. Use of subcontractors by the service provider should be prohibited without the prior approval of the fund.

A top-down compliance programme

Effective data protection starts with knowing your data, but in the era of mobile devices and cloud computing, identifying the full extent of a fund's personal data holdings can be difficult, as the databases are not always clearly marked out as such. A data audit should be conducted to establish a clear view of the data, both fund proprietary data and client-specific personal data.

Once the various data holdings have been identified, the next step will be to identify how any personal data was obtained and the purposes

Images: iStock Photo / leolintang

"Fintech solutions also raise data protection concerns that need to be carefully considered before they are adopted."

for which it is being processed. Understanding where personal data are being transferred to from the different points of collection is essential. Fund managers need to identify who in the organisation has access to personal data and whether they are empowered to send that data to authorised third party providers.

The Bill gives individuals the right to access personal data held about them and to request that any inaccurate data are corrected or deleted. Fund managers will need to have policies and procedures in place to manage these requests. The Bill also obliges businesses to cease processing personal data once the purposes for which that data have been collected have been exhausted. Prescribed data retention periods are not set out in the Bill but an analysis will need to be undertaken to determine how long data should be kept for. Similarly, it will be important to evaluate how personal data can be securely deleted once the purposes for holding it have been fulfilled.

Implementing a data protection compliance programme involves engagement with the right stakeholders across the organisation and creating an effective governance regime for approving, overseeing, implementing and reviewing the various policies. A coordinated chain of command should be developed, together with written reporting procedures, authority levels and protocols including seeking and complying with legal advice. The appointment of official roles such as a data protection officer is also recommended.

Compliance training will be required for personnel at all levels, including key external service providers, to emphasise the importance of compliance to the fund. Serious misconduct should be addressed with appropriate disciplinary action, regardless of seniority. The compliance programme should be reviewed regularly reflecting changes in law and regulation, changes in the data being collected and used and changes in technologies and operating procedures.

The growing threat of cyber crime

The funds industry represents an attractive target for cyber criminals. Not only are large sums of money being collectively managed by the industry, but often the size and operating structure of most funds does not afford them the resources required to invest in the people and IT infrastructure needed to counter increasingly sophisticated cyber attacks. As funds outsource a significant part of their day-to-day operations to external service providers, these transfers leave them vulnerable to attack. Cyber criminals can easily identify and exploit weak links in the flow of information between the fund and its external providers.

Data that may have been anonymised or aggregated by a fund will still require careful handling. The rise of social media and the increase in online public data sources means cyber criminals are now easily able to "re-identify" individuals by combining that information with the anonymised or aggregated datasets.

Portfolio-level information received in connection with due diligence and investment activities is often provided on a confidential basis. Non-disclosure agreements entered in connection with a potential investment opportunity should be read carefully to ensure that fund managers are not deemed to be in breach as a result of an unintentional disclosure of confidential information arising from a cybersecurity attack.

Data protection and new technologies

Financial technologies (fintech) are emerging technologies that have the potential to supplement or disrupt the financial services industry. Funds tend to be early adopters of these new technologies. As Cayman presses forward with its ambition to be a leading regional technology hub, fintech will soon become a key point of focus, for market participants and regulators here. Fintech solutions also raise data protection concerns that need to be carefully considered before they are adopted.

In the financial services industry, blockchain, or distributed ledger technology, is starting to be used to centralise a number of back-office and compliance functions. Blockchain is designed to keep a permanent, immutable record of all transactions that have taken place, but this is at odds with the requirement under the Bill to securely delete all personal data once the purpose of use has been fulfilled. As users of the ledgers are often anonymous, there is also the potential for criminal organisations to apply powerful data analytics to these datasets to match data that appear to be clear of personally identifiable information to those which are not, thereby allowing the re-identification of individuals from that data.

The attraction of flexible working has led to a growth in the popularity of "bring-your-own-device" (BYOD) policies. While some organisations are issuing smartphones and tablets for employees, other employees may be using their personal devices for business purposes without approval. Where BYOD is offered, a careful balance needs to be struck between employee satisfaction and protecting personal data.

Funds should put in place a clear BYOD strategy that sets out minimum do's and don'ts for using a device. There should be a clear segregation of enterprise data which should at all times be under the control of the fund. Data should be encrypted and the fund should have the ability to remotely access, monitor and wipe the data and prevent data access from third party apps.

Protecting personal data is now business-critical for funds. Even if monetary losses are not sustained as a result of personal data being mishandled, the reputational damage to a fund following a breach could be devastating.

Sailaja Alla is a partner at Appleby's Cayman Islands office. She can be contacted at: salla@applebyglobal.com

Peter Colegate is a senior associate at Appleby's Cayman Islands office. He can be contacted at: pcolegate@applebyglobal.com