GDPR: THIS TIME, IT'S PERSONAL

The European Union's new General Data Protection Regulation will have wide-ranging implications for the funds industry, as Philip Dickie and Tamarin Wilson from Harbour explain.

To remain relevant to modern privacy needs and bring its data protection laws into the 21st century, the EU has issued the General Data Protection Regulation (GDPR)—a broad data privacy regulation with tougher penalties, increased data protection accountability, and extended rights for individuals.

The territorial scope of the GDPR is vast; it will apply to all EU-based organisations which process personal data, and non-EU based organisations where their data processing activities relate to offering goods or services to data subjects (natural persons identified or identifiable as EU citizens or residents) or monitoring data subjects' behaviour insofar as their behaviour takes place in the EU.

The effective date of the regulation is May 25, 2018, and non-compliance may result in fines up to the greater of €10 million ($12.3 million) or 4 percent of annual global gross revenue.

Although the core provisions of the GDPR focus on curbing unauthorised access to, or unapproved use of, personal data by large tech companies, data aggregators and mass marketing firms, the GDPR's extensive remit will also affect the investment fund industry in a direct way. The regulation aims to reinforce current policies and enhance the development of a risk-based framework built around the individual's right to protection of privacy.

In an investment fund context, investors provide personal information to funds and their managers for various purposes, including to comply with anti-money laundering policies and procedures. Investment managers, administrators and other fund service providers will need to map all the ways in which personal data is used in their firms, and consider their responsibilities when processing personal data in their role as a data controller or a data processor, as the categorisation thereof determines their regulatory obligations.

A data controller is any natural or legal person who, alone or jointly with others, makes decisions regarding the purpose, conditions and means by which personal data is collected and processed, whereas a data processor is any natural or legal person who engages in processing data on behalf of the controller.

iStock Photo / akindo

> "The fund directors have to ensure that the investment manager, the fund administrator and other fund service providers are aware of their responsibilities."

The investment manager

Investment managers with a presence in the EU or with EU investors will typically be considered data controllers and be held accountable for fair and transparent data processing. Prior to, or at the point of, data collection the investment manager must disclose to the data subject the purpose of processing their personal data, the data subject's privacy rights and the manner in which they can exercise their rights.

Further obligations include ensuring that the investor has provided clear consent, by statement or an affirmative action, to use the data on a purpose-by-purpose basis and investors must be made aware that they may withdraw their consent at any time. This consent will be relied upon to demonstrate the legal basis for processing the data. Subscription documents should be amended to incorporate these requirements.

Ongoing responsibilities of investment managers, as controllers of investor data, will be to ensure that the appropriate level of technological and operational security is applied to protect the privacy of the data, and measures are implemented to remove irrelevant or excessive data which is no longer necessary to achieve the processing objective.

If a security breach occurs which is likely to risk the rights and freedoms of the data subject, a data protection authority must be notified within 72 hours of the breach. Investment managers must also implement processes to address accidental loss, unauthorised access, alteration, or destruction of personal data stored. Representations should be received from data processors, including administrators, to provide the manager with assurance that GDPR obligations are being met.

The fund

Fund boards and general partners must understand the regulation and its impact on each fund, as the fund is likely to be a controller of personal data as well. The fund directors have to ensure that the investment manager, the fund administrator and other fund service providers are aware of their responsibilities in relation to the requirements of GDPR and that they have implemented processes to ensure compliance.

As the GDPR requires internal governance for data protection, those charged with governance must ensure that investor data is protected by safeguards and controls within a robust framework where data is controlled, processed and retained in a secure environment.

The administrator

Fund administrators should perform an analysis for each fund structure, but as a general guide, fund administrators will be regarded as data processors as it relates to the processing of investor data on behalf of the data controller. As data processors, administrators must ensure that no processing of data is performed which is not clearly defined in the administration agreement or per instructions received from the data controller.

The GDPR stipulates mandatory requirements for the content and instructions of processing agreements and administration agreements must clearly set out the type of data being processed, the duration of the processing, the nature and purpose of processing, and the obligations and rights of the data controller and processor. Processes may not be delegated or outsourced without the prior consent of the data controller.

Administrators should ensure they have specific controls relating to data processing, data transfers, and data security procedures, and incorporate these controls in their system and organisation control reports. Administrators with more than 250 employees must keep prescribed, detailed documentation recording all their processing activities. A "one-stop shop" mechanism may be applied for administrators operating across multiple EU jurisdictions, whereby the main EU established office (usually the EU head office) may be elected as a lead supervisory authority which provides a central point to ensure effective enforcement of GDPR compliance, and consistency in addressing privacy related issues.

The data subject

The expanded data subject rights under GDPR include the right to be forgotten, the right to restrict processing, and the right to portability of data. It is important to note that the right to be forgotten does not supersede any legal requirements relevant to document retention for the fund.

From an investment funds perspective, the right to be forgotten may be the most problematic to address, due to the complexity of identifying all channels where personal data has been stored, including emails, printed documents, archives, file backups, etc.

Practical and precautionary measures within a compliance framework must be clearly documented to address the risks of a data subject exercising her/his right to be forgotten. Where there is an inability to meet the requirements, reasons for not doing so in respect of the impracticality or financial burden should be included.

Conclusions

Although the industry awaits further implementation guidance, precedent, and enforcement examples, the focus on personal data privacy is becoming strategically important and a 'wait-and-see' approach may lead to reputational harm or loss of competitive advantage as investor demand for privacy rises. Achieving personal data privacy means developing an evolving risk-based approach which is continuously assessed, and the main focus for compliance starts with a clear understanding of the risks and associated mitigants, rather than a check-the-box approach. ■

Philip Dickie is a director at Harbour. He can be contacted at pdickie@harbour.ky

Tamarin Wilson is a manager at Harbour. She can be contacted at: twilson@harbour.ky