Compliance matters: GDPR and investment funds

February 2018

In the ninth in a series of regulatory columns in Compliance Matters by experts in Guernsey's legal sector, Collas Crill Senior Associate in the Corporate and Commercial team, Gareth Morgan, discusses how the EU General Data Protection Regulation (GDPR) will affect investment fund structures.

GDPR is the current office 'crusade du jour' in many a financial, legal or investment management firm here in Guernsey. The principal tenets of the GDPR will be effective in many offshore jurisdictions via the extra-territorial effect of the regulation itself. In Guernsey, the Data Protection (Bailiwick of Guernsey) Law, 2017 will match the essential safeguards of personal data as set out in the GDPR, so that Guernsey maintains its current status as an 'adequate' jurisdiction, internationally.

The GDPR will affect all firms dealing with the personal data of EU citizens. While we may profess to understand its aims (stronger protections for personal data across the EU and those jurisdictions dealing with the EU), putting it into practice will require some thought when it comes to revising service provider's processes and procedures. Particular markets will face unique challenges in terms of compliance with the GDPR and the DP Law; this article takes a brief look at the investment funds sector.

Data Protection Principles

The DP Law will revise the fundamental principles of data protection, which are in line with the GDPR, namely that data is required to be processed:

- Lawfully, fairly and transparently
- In accordance with specified, explicit and legitimate purposes
- Only to the minimum extent necessary
- Accurately
- Stored no longer than is necessary for its purpose
- With integrity and confidentiality
- With accountability (by the controller/processor)

So what does this mean for a run-of-the-mill investment fund structure? Investment funds can be complex animals, so it is not always immediately obvious which persons, companies, service providers, etc, might be engaged in the controlling or processing of personal data for the purposes of GDPR and the DP Law and indeed what personal data they may hold or need to hold.

When an investor applies to subscribe for an investment in a fund, they will typically be required to provide their name, date of birth, postal address (and proof thereof), payment details and tax residency (in accordance with established anti-money laundering and "know your client" policies in place from time to time).

This is a relatively short list of requirements (painful as it may be to have to deal with at times), but consider what this involves in terms of handing over personal data: photo identification, utility bills with personal addresses, disclosure of source(s) of wealth/funds, employment details, dependents, investment profile information and more.

This is sensitive data that must be respected by the party or parties collecting it. And it does not necessarily stop at investor data: an investment manager set up alongside a fund will have obligations under GDPR and the DP Law with regard to personal data on the investment manager's employees.

Who are the data controllers/processors in an investment fund context?

Investment funds usually operate under the supervision of a board of directors, who will often delegate certain roles and powers to an investment manager (unless the fund is self-managed). In the context of data protection legislation, the investment manager, the fund itself and the relevant administrator could likely be construed as ‘data controllers’.

Additionally, either the fund board or the investment manager will appoint a range of other service providers depending on the type of fund and its needs. For a single investment structure you may have, in addition to an investment manager, a transfer agent, distributor, custodian and a company secretary.

Such service providers would generally be considered to be ‘data processors’. Some of those service providers may well outsource certain functions to subsidiaries or third-party agents, further widening the net of potential data processors.

An investor will invariably provide some or all of the information discussed above to one or more of these service providers, either in order to abide by the contractual obligations of investment into the fund (which are usually set out in the information memoranda and subscription documents), or to comply with the ‘know your customer’ and anti-money laundering policies and procedures of the relevant service providers.

It is also likely that such service provider will need to share investor data between themselves to satisfy their respective roles within the structure. This personal data will be processed and stored by these service providers for their own purposes and on behalf of the fund.

Coming back to the fund itself, the board of directors will of course need to be comfortable that, at each level where data is controlled, processed, stored etc, there are sufficient safeguards and processes in place for the proper governance and protection of the personal data of investors.

As a result, broad and permissive delegation powers often found in investment management and administration agreements will need to be made subject to (among other things) the delegate's ability to demonstrate effective compliance with the GDPR and the DP Law.

What can or should be processed?

With regard to the type and substance of the data held or to be held at each level in a fund, the relevant key principle from the DP Law is that the data should be:

"*adequate, relevant and limited to what is necessary for the purposes for which it is processed*".

This needs to be considered carefully on a service-by-service basis. When it comes to investor information what is "necessary" for, say, an administrator, might not be justifiably necessary for a distributor or an investment advisor, so what information can be passed between such entities becomes less clear.

Service providers will need to be able to demonstrate clear, affirmative action by the 'data subject' (i.e. the investor) that they have freely consented to the processing of their personal data.

A general indication of consent from the investor set out in a subscription form will not be sufficient (the consent must be clear and specific) and cannot be used as a blanket permission to control a person's data.

As consent cannot be withdrawn, it should not be obtained where the data controller/processor has a 'specific, explicit and legitimate purpose' in collecting and processing the data, such as for compliance with anti-money laundering legislation. Many standard form fund subscription agreements will as a result need a significant upgrade in this area to account for the specificity required when it comes to investor consent and information rights.

Service providers classed as data processors (these could take the form of agents, sub-custodians and investment advisors) will be directly liable for their activities relating to the processing of personal data.

They will no longer be able to pass on responsibility to the relevant data controller. Further, the precise remit of the data processor with regard to processing investor data will need to be set out in clear instructions from the data controller in the relevant service contract.

Additionally, data subjects must be informed of their rights under the DP Law and GDPR and how to exercise them. A logical place for this disclosure will be in the fund's information documents (scheme particulars, prospectus, etc). given this is the prime source of information on a fund from an investor perspective.

Who is responsible?

As mentioned above, data controllers and data processors have direct liability for their activities regarding personal data, with their own responsibilities for implementing appropriate safeguards. However, the board of a fund which has appointed these service providers should maintain appropriate oversight and get comfortable that safeguards are in place at every level.

The penalties for breaching the DP Law are more significant than under the existing data protection regime, with fines of up to £300,000 or 10% of global annual turnover (up to a limit of £10 million) possible for breaches of the fundamental principles established under the DP Law.

That being said, the board of a fund will invariably rely upon their administrator for the bulk of their data processing, particularly as it would be part and parcel of the administrator's on-boarding process for investors. With this in mind, administrators may well find themselves under particular scrutiny when pitching for fund business; a service provider who can demonstrate the ability and infrastructure to comply with the GDPR in an efficient and cost-effective manner is going to have a competitive advantage.

A data revolution in the funds industry?

Data is fast-becoming on of the most prevalent, and valuable, commodities on the planet. As regulation evolves, so must the market. When considering the impact of GDPR and related legislation on funds, the directors of said funds, as well as each service provider, will need to assess their own obligations and every player needs to understand its responsibilities.

The being said, the GDPR and DP Law have, in effect, tinkered with an established regime to make it tighter, more transparent and fairer for data subjects. But the basic framework, with which investment funds and service providers have all been complying for many years, is still there.

So a revolution this is not, and provided the players involved commit to the early adoption of sensible procedures and documentation to ensure investor data is appropriately used and safeguarded, it can be business as usual.

An original version of this article was first published in Compliance Matters, January 2018.

For more information please contact:

Wayne Atkinson

Partner // Guernsey

t:+44 (0) 1481 734225 // *e:*wayne.atkinson@collascrill.com