Privacy and data protection: Bermuda

Stephanie Sanderson, of BeesMont, identifies the nuances of the incoming PIPA and GDPR regulation

2018 is expected to be a big year for privacy and data protection in Bermuda. The Personal Information Protection Act (Pipa) is set to come fully into force later this year and its full implementation is highly anticipated, particularly in light of the introduction of the EU's General Data Protection Regulation (GDPR) which applies from May of this year. Pipa is critical to ensuring Bermuda's reputation as a leading international offshore centre is safeguarded in the digital age we now operate in. GDPR and Pipa have each been developed to address the era of big data as well as mobile technology.

While Pipa draws particular similarities with GDPR and Canadian privacy legislation, it is important to understand that Pipa complies with international best practice and relies on global data protection principles. Pipa was developed with the intention that an application for a finding of 'adequacy' can be made to the EU. Given the nature of Bermuda's international business sector, a finding of 'adequacy' would be viewed as a major advantage for the jurisdiction and would ensure that Bermuda has the ability to transfer personal information freely with the EU.

Being prepared for privacy and data protection law changes requires a measured and informed approach.

GDPR's impact on Bermuda

Effective 25 May 2018, GDPR represents a major update of the current EU data protection and privacy laws replacing current rules governing the collection, storage and processing of personal data.

Stephanie P. Sanderson
Partner, corporate department at BeesMont Law

STEPHANIE P. SANDERSON is a partner at BeesMont Law Limited. She practices in all areas of corporate and commercial law with particular emphasis on M&A, investment funds, insurance, finance, restructurings, and cross-border transactions, as well as international tax, regulatory and compliance (including AML/ATF), data protection and privacy law.

Key drivers of GDPR are the granting of additional rights for individuals to control their data (including the "right to be forgotten"), imposing new and enhanced responsibilities on companies and other organisations for safeguarding the data they process, and harmonising standards across the EU and beyond to help create a "single digital market".

An important feature of GDPR is its purported extraterritorial effect. GDPR will apply to companies outside the EU if they are processing data of EU data subjects, providing services to EU citizens or monitoring behaviour that takes place in the EU. The impact of GDPR is therefore anticipated to be wide-ranging.

GDPR sets out six lawful reasons for using personal data. One or more of these reasons must exist in order to permit lawful use of personal data and there cannot be "back-up" reasons for use. It is important to determine the reason(s) for use of personal data and maintain that position consistently.

GDPR distinguishes between 'data controllers' and 'data processors', placing specific obligations on each. This distinction between data controllers and data processors must be determined on a case-by-case basis.

Breaches of GDPR can result in fines of up to €20m ($23.4m) or 4% of a firm's global turnover, whichever is higher.

Bermuda's privacy legislation – Pipa

When fully in force, Pipa will apply to every organisation (any individual, entity or public authority) that uses personal information in Bermuda where that personal information is used by automated means or are part of a structured filing system. Third-party transfers are permitted but the organisation engaging the third party remains ultimately responsible for ensuring compliance with Pipa.

Organisations will need to designate a representative (privacy officer) for the purposes of compliance with Pipa. The privacy officer will have primary responsibility for communicating with the privacy commissioner appointed pursuant to Pipa. Pipa allows for a group of organisations under common ownership or control to appoint a single privacy officer (provided that a privacy officer is accessible from each organisation).

Pipa imposes a standard of reasonableness on organisations for meeting its responsibilities under Pipa. Pipa also imposes a proportionality test such that organisations must ensure personal information is adequate, relevant and not excessive in relation to the purposes for which it is used.

Breaches of Pipa can result in imprisonment or fines of up to $250,000.

Interplay between GDPR and Pipa

GDPR uses various key definitions which do not necessarily have a Pipa equivalent term although many of the principles between GDPR and Pipa are well aligned.

Under GDPR, a 'data subject' means an identified or identifiable natural person and under Pipa an 'individual' means a natural person. In a funds context this would likely relate to investors of the fund or directors, officers and employees of an investment management company, for example.

Under GDPR, 'personal data' means any information relating to a data subject, who can be identified, directly or indirectly in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Under Pipa 'personal information' means any information about an identified or identifiable individual. It is also worth noting that Pipa includes specific provisions for 'sensitive personal information' defined as any personal information relating to an individual's place of origin, race, colour, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information or genetic information.

For example, this might include information included on director and officer registers, beneficial ownership registers and share registers, Know Your Client (KYC), Anti-Money Laundering (AML), Anti-Terrorist Financing (ATF) or other compliance documentation, as well as data and information on directors and/or employees of investment management companies. This can also potentially relate to online identifiers that can be used to identify an individual.

Under GDPR, a 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Pipa does not have an equivalent term but imposes obligations on each organisation. This could capture the investment management company, fund or a fund umbrella, for example.

GDPR and Pipa have each been developed to address the era of big data as well as mobile technology

Under GDPR, a 'processor' means any natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Again, Pipa does not have an equivalent term but, as above, imposes obligations on each organisation and it also includes third party provisions. This may impact fund administrators, paying agents, depositaries, distributors or any other delegates or agents that receive personal data in relation to investment funds. Any entities processing fund subscriptions or carrying out AML/ATF/KYC work for a fund may be caught here.

Recommended steps

A holistic approach is advisable so that all systems, policies and procedures, processes and documentation are reviewed for compliance with applicable privacy and data protection obligations. An information audit and data mapping exercise is advisable and organisations should ensure they are properly educated on the relevant laws.

Fund documentation should be reviewed in light of obligations under the appropriate privacy regimes. In particular, fund subscription documents or applications should contain relevant information with respect to the use of personal data as well as consents for same. Prospectuses and websites will also likely need updating once reviewed through this lens.

Relevant service provider contracts and any other relevant third-party contracts should be reviewed and updated, for example to clearly delineate the split between the data 'controller' and data 'processor' (or 'third party') relationship in administration agreements. Employment contracts will need to be revised as applicable – for example, in relation to employees of an investment management company.

Data retention policies will need to be assessed and/or implemented given that any personal information used should be accurate and kept up to date to the extent necessary for the purposes of its use. Personal information should not be kept for longer than is necessary for its specific use. Different types of personal data may require different retention periods which should be considered as part of the holistic analysis undertaken by any organisation. HFM

Further information

This article is intended for informational purposes only and is not a substitute for legal advice. Should you have any questions or would like to discuss the above, please contact Stephanie P. Sanderson, Partner – spsanderson@beesmont.bm.