Article

GDPR and the Cayman Data Protection Law for Insurance Managers (and clients)

Authors: Rob Humphries, Counsel | **Rory O'Connor,** Associate

The General Data Protection Regulation 2016/679, or "GDPR", is a set of EU regulations aimed at the protection of personal data and privacy of natural persons (not corporations) based within the EU. The GDPR has extraterritorial effect in that it applies to the processing of personal data of persons who are situated in the EU by a controller or processor (such as a captive or insurance manager) not established in the EU where the processing activities are related to the offering of goods or services, or the monitoring of the data subject's behavior within the EU.

Does the GDPR apply to Cayman captives and insurance managers?

Yes, possibly. However, it's not very common to find Cayman captives and insurance managers who are in scope for GDPR purposes because, firstly, the vast majority of Cayman's captive insurance business originates from the USA. As a result, it's not often that a Cayman captive or insurance manager will find themselves controlling or processing the personal data of any natural person situated within the EU. Secondly, it's not often that a Cayman captive or insurance manager could be said to be processing the personal data of a natural person situated within the EU in relation to the offering of goods or services or the monitoring of that person's behaviour, though this may occur from time to time. An example of which might be where personal data of an EU based insured is processed by the captive or the manager in relation to certain travel, health or life insurance policies.

What is the Cayman Islands' position on the protection of personal data and privacy?

Cayman has sensibly decided to follow suit with the EU and numerous other jurisdictions around the world by enacting its own data protection regime, largely in line with the data protection principles set out in the GDPR. The Cayman Islands Data Protection Law (DPL), 2017 came into force on 30 September, 2019 and serves to address the genuine need for protection of personal data within the Cayman Islands, and also to meet international standards on data protection in an effort not to impede the transfer of personal data between Cayman and other jurisdictions for legitimate purposes. The DPL will affect any individual or organisation established in Cayman which processes personal data, even where that data is being processed outside of Cayman.

What is personal data and who is deemed to control or process it under the DPL?

The DPL proposes restrictions on the 'processing' of any 'personal data' relating to any 'data subject' by or on behalf of a 'data controller'. In this context:

You are processing personal data if you obtain, record, hold or carry out any operation(s) on personal data, such as organising, adapting, altering, retrieving, consulting or using it, disclosing the personal data by transmission, dissemination or otherwise making it available, or, aligning, combining, blocking or destroying the personal data.

Personal data is any data relating to a living individual who can be identified. It includes, but is not limited to, their address, any online identifier, their appearance, psychological, genetic, mental, cultural or social identity, or the data controller's (or any other person's) opinions of or planned action towards them. In the context of the operations of a Cayman captive insurer that would likely include, but not be limited to, data on shareholders and affiliates, programme participants, directors, officers and individual insureds under the

programme (such as with life and health policies). For insurance managers it would likely include all of the above in relation to the captives managed but also their own staff and employees.

A data subject is any living individual who is either identified or who might be identified directly or indirectly. Some examples of potential data subjects in the context of the operations of Cayman captives and insurance managers are referenced in relation to "personal data" listed above.

A data controller is a person or legal entity established in the Islands who, alone or jointly with others determines the purposes, conditions and manner in which any personal data are, or are to be processed for their Cayman operations. Where a data controller is not established in Cayman, the data controller will be the Cayman based representative who must be appointed.

What are the rules?

There are eight 'Data Protection Principles' with which the data controller must comply. They are summarised as follows:

Fairness

Personal data must be processed fairly and for a legitimate purpose. In the context of the operations of a captive insurance company or insurance manager this will likely mean that, at a minimum, the identity of the data controller and the purpose for which the data is being processed has been disclosed to the data subject and the consent of the data subject has been given for the personal data to be processed.

Lawfulness

Personal data shall be obtained only for one or more specified lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

Data minimisation

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are collected or processed.

Accuracy

Personal data shall be accurate and, where necessary, kept up to date.

Storage limitation

Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

Rights respected

Personal data shall be processed in accordance with the rights of data subjects under this law.

Integrity and confidentiality

Appropriate technical and organizational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

International transfer restrictions

Personal data shall not be transferred to a country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

In addition to compliance with the above principles, other material provisions of the DPL that captives and their managers should be aware of include subject access rights to their personal data and to be given information about how it is being processed. This includes the data subject's right to give notice to a data controller to cease processing their data. There are also important provisions in relation to the procedures to be followed by data controllers in the event of a data security breach. Captives and their managers should have procedures in place to deal with such requests and address the rights of data subjects within the specified time periods.

Are there any exemptions?

Yes, there are several exemptions, but none that are likely to apply to the operations of Cayman captives or their managers.

What are the sanctions for non-compliance?

The DPL allows for the imposition of various fines not exceeding $250,000 and/or imprisonment not exceeding five years for specified contraventions under the law.

What steps will need to be taken towards compliance with the DPL?

The first step will be to identify what personal data is handled and why, the types of data and the types of data subject. From this you can understand which data protection legislation applies to your business (is it just the DPL or is GDPR also relevant?) and begin to identify the work that needs to be done to bring it into compliance. It is then a case of engaging key people from the business (the captive board and the insurance manager) and outside advisors to develop and implement a plan for compliance.

Conyers has advised some of Cayman's leading managers and their clients on DPL compliance and implementation. We offer tailored advice on the application of the DPL to your business with recommendations for compliance and implementation including

- Drafting staff Guidance Notes with recommendations for compliance and implementation.
- Initial and ongoing staff training and required.
- Provide Data Policy Handbook including:
    - Data Breach Procedure Policy;
    - Remote and Mobile Working Policy;
    - Clean Desk Policy;
    - Subject Access Request Procedure; and
    - Employee Transparency Policy.
- Review and update Privacy Policy Notices.
- Review Management Agreement and third party agreements as required.
- Drafting corporate authorisations documenting DPL implementation and compliance.

Authors:

Rob Humphries
Counsel
rob.humphries@conyers.com
+1 345 814 7793

Rory O'Connor
Associate
rory.oconnor@conyers.com
+1 345 814 7780

Cayman Insurance Contacts:

Derek Stenson
Partner
derek.stenson@conyers.com
+1 345 814 7392

Paul Scrivener
Independent Consultant
paul.scrivener@conyers.com
+44 7393 932337

Philippa Gilkes
Associate
philippa.gilkes@conyers.com
+1 345 814 7751