Article

Data Protection Law for Insolvency Practitioners ("IPs")

This article considers what an IP's role is in respect of the recently enacted Data Protection Law, 2017 ("DPL") and some practical considerations for IPs in the Cayman Islands when faced with managing personal data.

Authors: Paul Smith, Partner and **Róisín Liddy-Murphy,** Attorney

Introduction

The DPL came into effect as of 30 September 2019. The Office of the Ombudsman is Cayman's supervisory authority for data protection. The DPL applies to personal data processed by "data controllers" and "data processors". Cayman financial sector entities established in the Cayman Islands will generally be considered "data controllers", "data processors" or both. The DPL also applies to "processing" carried out by data controllers established within the Cayman Islands and to data controllers outside of the Cayman Islands that process personal data within the Cayman Islands. The DPL does not carve-out or exempt companies facing financial difficulties or in formal insolvency proceedings. As a result, the DPL applies to insolvent companies and any appointment taker such as an IP in formal insolvency proceedings.

Definitions under the DPL

The first step in ascertaining whether or not the DPL is applicable to an IP is to establish if the IP is a data controller or a data processor.

- A "*data controller*" is the person who alone or jointly with others determines the purposes, conditions and manner in which any personal data are, or are to be processed.
- A *"person"* includes any corporation, either aggregate or sole, and any club, society, association, public authority or other body, of one or more persons.
- A *"data processor"* is any person which processes personal data on behalf of a data controller but does not include an employee of the data controller.
- The term *"personal data"* means data relating to an identifiable living individual referred to as a *"data subject"*. The data subject does not need to be in the Cayman Islands.
- The term *"processing",* in relation to data, means obtaining, recording or holding data or carrying out any operation or set of operations on personal data.
- The term *"personal data breach"* means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data transmitted, stored or otherwise processed.

Under the DPL the data controller is responsible for ensuring that the eight data protection principles are complied with.

DPL issues in insolvency

IPs will need to consider carefully whether they could personally be categorised as data controllers and/or data processors upon their appointment. Generally under the DPL a service provider which performs an outsourced administrative or support function is more likely to act as a data processor, while service providers which provide more regulated professional services such as an IP are more likely to be treated as a data controller. It is important for IPs to conduct an analysis of how and what personal data will be processed during their appointment.

Justification for data processing

IPs as data controllers must ensure that they have a legal basis to process personal data. Under Schedule 2 of the DPL one of the lawful grounds for handling personal data includes complying with a legal obligation which in a formal insolvency would justify the IP's handling of the personal data. However, even though an IP may have a legal justification for the handling of such data they will still need to ensure that they are operating in compliance with the DPL. This can be challenging at a time when the financial entity they are appointed over, has limited resources to put towards compliance and therefore it is important that an IP understands its obligations from the outset to minimise the risk of a breach. Although there is no specific

requirement under the DPL for a data controller to have a formal internal data protection policy in place, it would be advisable for IPs to put in place their own policies and procedures for handling personal data. The Ombudsman takes the position that having documented policies and processes in place will be very helpful when a data subject exercises his or her rights, when a personal data breach occurs or in the event of an investigation by the Ombudsman.

Rights of data subjects

The DPL sets out a number of rights of individual data subjects. Amongst those, is an individual's right to access their own personal data and receive information about its use. IPs operating as data controllers will be under an obligation to comply with data subject access requests ("DSAR") within 30 days of a request and under the DPL they may not impose a fee to deal with a DSAR request except in exceptional circumstances. There are some limited exemptions to this right to access but generally IPs should be prepared and aware of their obligations if acting as a data controller, to disclose. Individuals also have a right to have inaccurate personal data rectified, blocked, erased or destroyed. An individual has the right to complain to the Ombudsman about any perceived personal data breach of the DPL and to seek compensation for damages in the courts.

Data security

The DPL seeks to place a greater control over how personal data is processed and stored. IPs acting as data controllers and/or data processors may find themselves facing potentially significant additional costs to implement appropriate protection measures if an entity's data is not sufficiently secured prior to their appointment in order to safeguard against the risk of a data breach when they assume control of the company.

Personal data breaches

A personal data breach can be broadly defined as a security incident that affects the confidentiality, integrity or availability of personal data. When a security incident takes place, a data controller must notify the Ombudsman and the affected data subject(s) of the personal data breach without undue delay and no longer than five days after the data controller was made aware of the personal data breach.

Retention Policies

Data retention policies or schedules list the types of information a data controller holds and for how long they hold it. The DPL does not dictate how long information should be kept. It is up to the data controller to justify this, based on its legal purpose for processing. IPs will only be permitted to retain personal data necessary to fulfil its legal obligation in a formal insolvency. Once the legal obligation is satisfied that information should be erased (deleted) or anonymised.

Conclusion

Under the DPL, IPs will need to consider carefully whether they could be categorised as a data controller and/or data processor from the outset of their appointment. When IPs assume control of an insolvent company they will often assume all the multiple categories of data of the business, including books and records, employee files, client lists and information about directors/ creditors. It is important for an IP to conduct an analysis and identify the information that it will be assuming control over and to understand how such information will be secured and processed during its appointment. If an IP is operating as a data controller it needs to ensure that it is responsive to data requests and that it is operating in full compliance with the DPL to avoid leaving itself open to complaints being submitted to the Ombudsman and the risk of damages being awarded against it. Such complaints could prove not only costly but could also damage an IP's professional reputation and undermine the trust of its creditors.

For more information on the **DPL** please reach out to your usual Conyers contact, or one of those listed below.

Speak to our experts:

Paul Smith
Partner
paul.smith@conyers.com
+1 345 814 7777

Róisín Liddy-Murphy
Attorney
roisin.liddy-murphy@conyers.com.
+1 345 814 7371