DATA PROTECTION LAWS OF THE WORLD

Cayman Islands

CAYMAN ISLANDS

Last modified 26 January 2023

LAW

The Data Protection Act (2021 revision) (**DPA**) is a Cayman Islands law, which first came into force on 30 September 2019. The DPA introduced the first legislative framework on data protection in the Cayman Islands.

Application

The application of the DPA turns on whether an organization is established in the Cayman Islands or has personal data processed in the Cayman Islands. Specifically, the DPA applies to a data controller in respect of personal data only if:

- the data controller is established in the Cayman Islands and the personal data are processed in the context of that establishment; or
- the data controller is not established in the Cayman Islands, but the personal data are processed in the Cayman Islands other than for the purposes of transit of the data through the Cayman Islands.

For these purposes, '*established in the Cayman Islands*' means:

- a body incorporated, or a partnership or other unincorporated association formed, under the laws of the Cayman Islands;
- a body registered as a foreign company under the laws of the Cayman Islands;
- an individual who is ordinarily resident in the Cayman Islands; or
- any other person who maintains (i) an office, branch or agency in the Cayman Islands through which the person carries on any activity; or (ii) a regular practice in the Cayman Islands.

A data controller not established in the Cayman Islands that processes personal data in the Cayman Islands is required to appoint a local representative established in the Cayman Islands who, for all purposes within the Cayman Islands, is the data controller and bears all obligations under the DPA as if it were the data controller.

DEFINITIONS

The DPA defines '**personal data**' as data relating to a living individual who can be identified, including data such as:

- the living individual's location data or online identifier;
- factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the living individual;
- an expression of opinion about the living individual; and
- any indications of the intentions of the data controller or any other person in respect of the living individual.

The DPA creates more restrictive rules for the processing of '**sensitive personal data**', which includes personal data consisting of a data subject's racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, physical or mental health or condition, medical data, sex life or commission or alleged commission of an offence or related proceedings.

Under the DPA the '**processing**' of personal data has an extremely broad meaning and includes obtaining, recording or holding data, or carrying out any operation on personal data.

Personal data may be processed by either a **data controller** or a **data processor**. The data controller is the decision maker, 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*'. The data processor '*processes personal data on behalf of a data controller*'. The obligations under the DPA are imposed almost exclusively on the data controller.

A '**data subject**' is an identified living individual or a living individual who can be identified directly or indirectly by means reasonably likely to be used by the data controller or by any other person.

NATIONAL DATA PROTECTION AUTHORITY

The supervisory authority under the DPA is the Office of the Ombudsman of the Cayman Islands (the **Ombudsman**), who has issued detailed guidance on the DPA, accessible on the Ombudsman's website at https://ombudsman.ky/data-protection.

The Ombudsman's contact details are as follows:

Office of the Ombudsman

PO Box 2252

Grand Cayman KY1-1107

CAYMAN ISLANDS

Email: info@ombudsman.ky

Telephone number: +1 345 946 6283

REGISTRATION

There is currently no requirement for a data controller or data processor to notify the Ombudsman of their role or complete any registration.

DATA PROTECTION OFFICERS

There is no requirement for organizations to appoint a data protection officer under the DPA, though this may be recommended for larger or complex organizations.

COLLECTION & PROCESSING

A data controller is responsible for compliance with a set of eight core principles which apply to the personal data that the data controller processes. A data controller is also responsible for ensuring that the principles are complied with in relation to personal data processed on the data controller's behalf.

Under these principles:

- Personal data must be processed fairly, lawfully and in a transparent manner;
- Personal data must be obtained for specified lawful purposes and not further processed in any manner incompatible with those purposes;
- Personal data must be adequate, relevant and not excessive in relation to the purposes;
- Personal data must be accurate and where necessary kept up-to-date;
- Personal data must not be kept for longer than is necessary for the purposes it was collected for;
- Personal data must be processed in accordance with the rights of data subjects under the DPA;
- Appropriate technical and organizational measures must be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data; and

- Personal data must 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.

For purposes of the first principle (fair and lawful processing), personal data will not be treated as processed fairly unless the data subject has, as soon as reasonably practicable, been provided with, at a minimum, the identity of the data controller and the purpose for which the data are to be processed. This is usually communicated in the form of a privacy notice.

In order for the processing to be considered lawful, the processing must be justified by reference to an appropriate basis. The legal bases (also known as lawful grounds) for processing personal data are:

- The data subject has given consent to the processing (where consent must be freely given, specific, informed and unambiguous and must be capable of being withdrawn at any time);
- The processing is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject with a view to entering into a contract;
- The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- The processing is necessary to protect the vital interests of the data subject;
- The processing is necessary for the administration of justice or the exercise of a function by a public authority or conferred under law or other function of a public nature exercised in the public interest; and
- The processing is necessary for the purposes of legitimate interests pursued by the data controller or a third party to whom the data is disclosed, except if the processing is unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Sensitive personal data

In order for the processing of sensitive personal data to be considered lawful, in addition to meeting one of the above legal bases, one of the following conditions must be met:

- The data subject has given consent to the processing (where consent must be freely given, specific, informed and unambiguous and must be capable of being withdrawn at any time);
- The processing is necessary for the purposes of exercising or performing a right or obligation conferred or imposed by law on the data controller in connection with the data subject's employment;
- The processing is necessary to protect the vital interests (i) of the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject; or (ii) of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;
- The processing is carried out by a not-for-profit body in certain limited circumstances;
- The information contained in the personal data has been made public as result of steps taken by the data subject;
- The processing is necessary for the purposes of legal proceedings, obtaining legal advice or otherwise establishing, exercising or defending legal rights;
- The processing is necessary for the administration of justice or the exercise of a function by a public authority or conferred under law; or
- The processing is necessary for medical purposes and is undertaken by a health professional or person who owes an equivalent duty of confidentiality.

Rights of the Data Subject

Right of access

Upon written request, a data subject is entitled to be informed by a data controller of whether their personal data are being processed by or on behalf of the data controller and, if so, to be given a description of such personal data together with prescribed information about how the data have been used by the data controller. A data subject is also entitled, upon written request, to a copy of their personal data and any information available as to the source of such personal data. A data controller is generally required to comply with such a request within 30 days.

Right to object to processing

A data subject is entitled, at any time by notice in writing, to require a data controller to cease processing, or not to begin processing, or to cease processing for a specified purpose or in a specified manner, the data subject's personal data. A data controller is required to comply with such a notice as soon as practicable and in any case within 21 days, unless the processing is necessary:

- for the performance of a contract to which the data subject is a party or the taking of steps at the request of the data subject with a view to entering into a contract;
- for compliance with a legal obligation to which the data controller is subject; or
- in order to protect the vital interests of the data subject.

In addition, data subjects have an unconditional right to require a data controller at any time to cease (or not to begin) processing their personal data for the purposes of direct marketing.

Rights in relation to automated decision-making

A data subject is entitled, at any time by notice in writing, to require a data controller to ensure that no decision taken by or on behalf of the data controller that significantly affects the data subject is based solely on the processing by automatic means of the data subject's personal data for the purpose of evaluating the data subject's performance at work, creditworthiness, reliability, conduct or any other matters relating to the data subject.

Where a decision that significantly affects a data subject is based solely on processing by automatic means, subject to certain exceptions, the data controller is required as soon as reasonably practicable to notify the data subject that the decision was taken on that basis, and the data subject is then entitled to require the data controller to reconsider the decision.

Right to rectification

The DPA includes an indirect right for individuals to have inaccurate personal data rectified, by making such a request to the data controller. There is no explicit obligation for a data controller to act on such a request, however data controllers are generally required under the principles to process data fairly and transparently and ensure that personal data is accurate and kept up-to-date.

Any person may make a complaint to the Ombudsman about the processing of personal data and the Ombudsman may order the data controller (among other things) to rectify, block, erase or destroy the relevant data.

TRANSFER

As set out in the eighth principle, transfers of personal data by a data controller or a data processor to countries or territories outside the Cayman Islands are only permitted where 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. This is to ensure that the level of protection provided by the DPA is not circumvented by transferring personal data abroad.

The Ombudsman has issued guidance stating that it considers the following countries and territories as ensuring an adequate level of protection:

- member states of the European Economic Area (that is, the European Union plus Lichtenstein, Norway and Iceland) where Regulation EU 2016/679 (the General Data Protection Regulation or "GDPR") is applicable; and
- any country or territory in respect of which an adequacy decision has been adopted by the European Commission pursuant to Article 45(3) GDPR or remains in force pursuant to Article 45(9) of the GDPR.

Other countries and territories may be deemed to have an adequate level of protection depending on various factors, which are to be assessed by a data controller, or a data controller may request authorization from the Ombudsman for a transfer.

The DPA also includes the following exceptions where the eighth principle will not apply to a transfer:

- if the data subject has consented to the transfer (where consent must be freely given, specific, informed and unambiguous and must be capable of being withdrawn at any time);

- where the transfer is necessary for the performance of a contract between the data subject and the data controller, or the taking of steps at the request of the data subject with a view to the data subject's entering into a contract with the data controller;
- the transfer is necessary for the conclusion of a contract between the data controller and a person other than the data subject, being a contract that is entered into at the request of the data subject, or is in the interests of the data subject, or for the performance of such a contract;
- the transfer is necessary for reasons of substantial public interest;
- the transfer is necessary for the purposes of legal proceedings, obtaining legal advice or otherwise establishing, exercising or defending legal rights;
- the transfer is necessary in order to protect the vital interests of the data subject;
- the transfer is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by a person to whom the data are or may be disclosed after the transfer; or
- the transfer is required under international cooperation arrangements between intelligence agencies or between regulatory agencies to combat organized crime, terrorism or drug trafficking or to carry out other cooperative functions, to the extent permitted or required under Cayman Islands law or an order of the Grand Court of the Cayman Islands.

SECURITY

The DPA is not prescriptive about specific technical standards or measures that must be taken to protect personal data. Rather, the DPA adopts a context-specific approach, requiring that appropriate technical and organization measures be taken, appropriate to the risks presented by the processing. A data controller should take into account the state of the art, costs of implementation, as well as the nature, scope, context and purpose of their processing.

Aspects to consider include:

- organizational measures, e.g. staff training and policy development;
- technical measures, e.g. physical protection of data, pseudonymization, encryption; and
- securing ongoing availability, integrity and accessibility, e.g. by ensuring backups.

BREACH NOTIFICATION

The DPA contains a general requirement for a personal data breach to be notified by the data controller to the Ombudsman and the relevant data subject(s). A personal data breach is a wide concept, defined as '*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed*'.

The data controller must notify a breach to the relevant data subject(s) and the Ombudsman without undue delay, and in any case no longer than five days after the data controller should, with the exercise of reasonable diligence, have been aware of the breach.

The same rules apply where a breach occurs at the level of a data processor. Accordingly, data controllers should contractually require their data processors to notify the data controller of a breach in a timely manner.

The notification must describe the nature of the breach, the consequences of the breach, the measures proposed to be taken by the data controller to address the breach and the measures recommended by the data controller to the relevant data subject(s) to mitigate the possible adverse effects of the breach.

ENFORCEMENT

A breach of the DPA constitutes a criminal offence, punishable on conviction to a fine of up to CI$100,000 (approx. US$125,000), imprisonment for a term of up to 5 years, or both.

In addition, the DPA empowers the Ombudsman to issue monetary penalty orders of up to CI$250,000 (approx. US$300,000) where the Ombudsman is satisfied on a balance of probabilities that there has been a serious contravention of the law by a data controller and the contravention was of a kind likely to cause substantial damage or substantial distress to a data subject.

Investigative and corrective powers

The Ombudsman is given wide investigative and corrective powers under the DPA, including to require the provision of information and to issue orders to carry out specific remediation activities.

Right to claim compensation

The DPA specifically provides for individuals to bring private claims against data controllers: any person who suffers damage by reason of a contravention by a data controller of any requirement of the DPA has a cause of action for compensation from the data controller for that damage.

Personal liability

The DPA explicitly provides for personal liability for offences committed by a body corporate where the offence is proven to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, any director, secretary or similar officer or any person purporting to act in such capacity. Where the affairs of a body corporate are managed by its members, this personal liability also applies to the acts and defaults of a member in connection with the member's functions of management.

ELECTRONIC MARKETING

The DPA applies to most electronic marketing activities as these will involve some use of personal data (e.g., an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent or the legitimate interests of the data controller. Where consent is relied upon, the strict standards for consent under the DPA are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to require a data controller at any time to cease (or not to begin) processing their personal data for the purposes of direct marketing (which includes direct electronic marketing).

ONLINE PRIVACY

There are no specific restrictions addressing online privacy beyond those generally applicable to the processing of personal data under the DPA. Personal data explicitly includes online identifiers.

KEY CONTACTS

Carey Olsen
www.careyolsen.com

Nick Bullmore
Partner
T +1 345 749 2000
nick.bullmore@careyolsen.com

Graham Stoute
Counsel
Carey Olsen
T +1 345 749 2014
graham.stoute@careyolsen.com

Jenna Willis
Counsel
Carey Olsen
T +1 345 749 2053
jenna.willis@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.