Conyers Dill & Pearman

How the Cayman Islands is Safeguarding Personal Data

Author:
Martin S. Lane, Partner

In June 2017, *The Data Protection Law* (the "DP Law") was published in the Cayman Islands Official Gazette. The DP Law will be brought into force by Cabinet Order. Related regulations and guidance are being settled such that we do not expect the DP Law to be brought into force before 2018.

The DP Law establishes a framework of rights and duties designed to safeguard individuals' personal data, balanced against the need of public authorities, businesses and organisations to collect and use personal data for legitimate purposes. The DP Law was developed in line with international best practices while ensuring that it reflects the specific needs of the Cayman Islands. It is based substantially on the *Data Protection Act, 1998* of the United Kingdom[1].

Most businesses record information in respect of individuals, particularly those who are employees, clients or suppliers, and the obligations under the DP Law will require a detailed review or establishment of policies and procedures in order to achieve compliance. Non-compliance may have serious ramifications.

The DP Law defines "personal data" very widely to include any data which enables an individual to be identified.

The DP Law is centred around eight data protection principles which require that personal data must:

1. be processed fairly and only when specific conditions are met, for instance where consent[2] has been given, where there is a legal obligation, or where it is necessary for the performance of a contract to which the data subject is a party. Additional conditions apply in respect of "sensitive personal data" (examples of which include, racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, health, sex life and offences);
2. be obtained only for one or more specified lawful purposes, and shall not be further processed in any manner incompatible with such purposes;
3. must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are collected or processed;
4. must be accurate and, where necessary, kept up to date;
5. must not to be kept for longer than is necessary for the purpose;
6. must be processed in accordance with the rights of individuals as specified under the DP Law;
7. must be protected by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage; and
8. not to be transferred abroad unless the country or territory to which it is transferred ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

[1] It does not reflect the EU's General Data Protection Regulation (2016/679), which will apply in the EU from 25 May 2018 following a two year transition period.

[2] "consent" is defined to mean any "freely given specific, informed and explicit indication of a data subject's wishes by which the data subject, either by a statement or by a clear act, signifies agreement to the data subject's personal data being processed."

It is hoped that the DP Law, when brought into force, will allow the Cayman Islands to be recognised by the EU Commission as providing adequate data protection[3].

Rights

The DP Law grants to living individuals referred to as ("data subjects") specific rights in relation to their personal data including, subject to specified limitations, the right to:

- be informed by a data controller whether their personal data is being processed;
- access their personal data and certain information about its use and source;
- require that processing of their personal data cease;
- require that processing of their personal data for the purpose of direct marketing cease;
- require that a decision which significantly affects him or her is not made solely by the processing by automatic means of personal data;
- seek compensation for damages caused by contravention of the data protection legislation;
- complain to the Information Commissioner where it appears that a violation has occurred; and
- seek from the Information Commissioner an order for rectification, blocking, erasure or destruction of inaccurate personal data and opinions based on such.

Duties

The DP Law imposes specific obligations on the persons who control the processing of personal data (so-called "data controllers" – see below), including the duty to:

- apply the data protection principles;
- respond in a timely fashion to requests from data subjects in relation to their personal data; and
- notify data subjects and the Information Commissioner of any personal data breaches.

If processing of personal data is to be carried out on behalf of a data controller by a data processor (not being an employee of the data controller), the data controller will not be regarded as complying with principle 7 above, unless the processing is carried out under a contract which conforms to specific requirements (to ensure compliance with the DP Law).

A person is entitled to be informed by a data controller whether the personal data of which the person is the data subject are being processed by or on behalf of that data controller and given stated particulars of such.

Application

The DP Law applies to a data controller established in the Cayman Islands if the data are processed in the context of that establishment. It also applies to a data controller who is not established in the Cayman Islands, but processes data in the Islands otherwise than for the purposes of transit of data through the Islands. Where a data controller is not established in the Islands, the data controller is required to nominate someone who is established in the Islands as a representative (which representative will themselves be liable as a data controller).

In order to be a "data controller", a person must be the person who, alone or with others, determines the purposes, conditions and means of the processing of personal data.

The regulated activity of "processing" personal data is very widely defined to include obtaining, recording or holding data, or carrying out any operation or set of operations (which is again very widely defined). It is difficult to envisage anything that an organisation might do with data that will not be considered to be processing.

Exemptions

In order to ensure that personal data can be used in appropriate circumstances, the DP Law recognises a number of exemptions to the obligations noted above, including national security, law enforcement, certain public functions, health care,

[3] The Council and the European Parliament have given the EU Commission the power to determine whether a third-country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into. The effect of such a decision is that personal data can flow from the EU and EEA member countries to that third country without further safeguards being necessary. The impact of the EU's General Data Protection Regulation on the prospects for such a determination are not yet clear.

education, social work, journalism, literature, art, research, history, statistics, information available under an enactment, legal proceedings, personal family or household affairs, honours, corporate finance, negotiations and legal privilege.

Data in respect of which legal professional privilege applies, in respect of certain types of trusts and in respect of wills made pursuant to the *Wills Law*, will be exempt from the subject information provisions of the DP Law[4].

Compliance and Enforcement

The Information Commissioner, currently tasked with oversight of the *Freedom of Information Law (2015 Revision)*, will assume a similar role for data protection, and will be given the powers, responsibilities and resources necessary to ensure the successful functioning of the legislation.

The Information Commissioner will have the power to:

- hear, investigate and rule on complaints;
- monitor, investigate and report on the compliance of data controllers under the law;
- intervene and deliver opinions and orders related to processing operations;
- order the rectification, blocking, erasure or destruction of data;
- impose a temporary or permanent ban on processing;
- make recommendations for reform both of a general nature and directed at specific data controllers;
- engage in proceedings where the provisions of the law have been violated, or refer violations to the appropriate authorities;
- cooperate with international data protection supervisory authorities;
- publicise and promote the requirements of the law and the rights of data subjects under it; and
- do anything which appears to be incidental or conducive to the carrying out of his or her functions under the DP Law.

The DP Law establishes a number of offences and penalties for failure to comply with the requirements of the DP Law, but also for:

- failing to notify the data subject and the Information Commissioner of a personal data breach;
- withholding, altering, suppressing or destroying information requested by the Information Commissioner;
- knowingly or recklessly disclosing information;
- obstructing a warrant, or making a false statement;
- unlawfully obtaining, disclosing, selling or procuring personal data;
- failing to comply with an enforcement or monetary enforcement order; and
- offences otherwise specified in Regulations.

The DP Law includes many detailed provisions and defined terms. In order to keep this paper short we have summarised several key terms and our summary may be an over-simplification. Reference should be made to the terms of the DP Law for more accurate particulars of its intended application.

What should a data processor be doing?

Although the DP Law is not yet in force, compliance with its requirements will take some considerable time to arrange and organisations are encouraged not to delay.

- Determine whether you are a "data controller" to whom the DP Law applies (Section 6). Organisations should be considering their operations in light of the DP Law and how personal data is processed to ascertain their position under the DP Law and whether any of the exemptions apply.

[4] Being, in short, the requirement of Principle 1 above for notice of the identity of the data controller and the purposes for which the data are to be processed to be given in order for data to be treated as being processed fairly and the right of a data subject to request in writing that he be informed by a data controller whether his personal data is being processed and, if so, to be given details of such.

- Determine whether the personal data that you are processing is "sensitive personal data" (per Section 3) in which case the first data protection principle also requires compliance with at least one of the conditions in Schedule 3 to the DP Law. Employee data often includes information about an employee's health and/or ethnic background and, as such, will comprise sensitive personal data.
- If you are a data controller that is not established in the Cayman Islands[5] and the data processing in the Cayman Islands is not only for the purposes of transit of the data through the Cayman Islands, then you must nominate someone who is established in the Cayman Islands to be your representative (Section 6).
- Understand the data protection principles in Part 1 of Schedule 1 of the DP Law and the required interpretation of those principles established by Part 2 of Schedule 1 to the DP Law, which, pursuant to Section 5(4), you are obliged to comply with in relation to personal data that are processed on your behalf.
- Allocate responsibility for compliance with DP Law obligations to a senior member of the management team.
- Put in place policies and procedures to:
    - ensure that data maintained is not excessive in relation to the purposes for which it is collected, is processed fairly and is used for a legitimate purpose which has been notified to the data subject;
    - validate information held about data subjects;
    - ensure that separate consent is sought where there are changes to the purposes for which data is obtained;
    - be effected in the event of a personal data breach (requiring prompt notice to the Commissioner and to affected data subject(s) - see Section 16);
    - enable a response to be compiled promptly (and in any event within 30 days) to a request made by a data subject (per Section 8(4)) for information regarding the data subject's personal data and the processing thereof – which, subject to limited exceptions, is required to be provided by data controllers per Section 8(1), (2) and (3);
    - ensure that processing of personal data ceases, does not begin, or ceases to be processed for a specified purpose or in a specified manner, if so required by a notice from a data subject in accordance with Section 10;
    - ensure that processing of personal data ceases once the purposes for which the data was collected have come to an end and to ensure secure deletion;
    - ensure that the processing of personal data for "direct marketing" ceases or does not begin following receipt of a notice from a data subject in accordance with Section 11;
    - ensure that data obtained via the business' online portal is retained only after requisite notices and consents have been given to and by data subjects;
    - inform clients, employees and other data subjects about data held in respect of them and the purposes for which such data is processed; and
    - ensure (unless other cases in Schedule 2 (and 3, where applicable) to the DP Law apply) that consent of the data subject is obtained when data is collected[6].
- Ascertain whether you use the services of data processors (e.g. for pay-roll processing) and, if so, consider whether the contractual documentation contains adequate and appropriate contractual protection relevant to your obligations in respect of the data under the DP Law (see Section 5(4)) and whether the contractor's systems are secure.
- Ensure that you do not transfer personal data to a country or territory other than one which ensures an adequate level of protection (per the 8th data protection principle, subject to the exceptions in Schedule 4).

For additional information, please contact your usual Conyers Dill & Pearman representative.

[5] Noting that a Cayman Islands registered foreign company is to be treated as established in the Cayman Islands per section 6(3).

[6] It should be noted that, (i) obtaining consent does not of itself mean that the processing is necessarily fair (as is required by the first data protection principle) and (ii) in order to comply with the second data protection principle, the purposes for which the personal data are to be processed will need to be "specified" (in a so-called "privacy notice" within an information section which often has a heading along the lines of "How we use your information". A privacy notice should also identify the data controller).

AUTHOR:

MARTIN S. LANE
PARTNER
martin.lane@conyersdill.com
+1 345 814 7395

GLOBAL CONTACTS:

FAWAZ ELMALKI
DIRECTOR
HEAD OF DUBAI OFFICE
fawaz.elmalki@conyersdill.com
+9714 428 2900

CHRISTOPHER W.H. BICKLEY
PARTNER
HEAD OF HONG KONG OFFICE
christopher.bickley@conyersdill.com
+852 2842 9556

LINDA MARTIN
DIRECTOR
HEAD OF LONDON OFFICE
linda.martin@conyersdill.com
+44(0)20 7562 0353

ALAN DICKSON
DIRECTOR
HEAD OF SINGAPORE OFFICE
alan.dickson@conyersdill.com
+65 6603 0712

ABOUT CONYERS DILL & PEARMAN

Conyers Dill & Pearman is a leading international law firm advising on the laws of Bermuda, the British Virgin Islands, the Cayman Islands and Mauritius. Conyers has over 130 lawyers in eight offices worldwide and is affiliated with the Conyers Client Services group of companies which provide corporate administration, secretarial, trust and management services.

For further information please contact: media@conyersdill.com