mourant

GUIDE

The Cayman Islands Data Protection Act, 2017

Last reviewed: December 2020

The Data Protection Act, 2017 and the Data Protection Regulations, 2018 came into force on 30 September 2019. Persons established or processing personal data in the Cayman Islands must ensure that they are compliant with the data protection regime.

2021934/76166093/2

1 Introduction

The Data Protection Act, 2017 (the **DPA**) came into force on 30 September 2019, together with the Data Protection Regulations, 2018 (the **Regulations**). Persons established or processing personal data in Cayman Islands must ensure that they are compliant with the DPA's requirements.

This Guide aims to provide readers with a basic understanding of Cayman's data protection legislation. The DPA does include a number of, sometimes conceptually difficult, defined terms and, for ease of reference, certain of those definitions have been duplicated in Schedule 1 to this Guide. We also refer readers to the Guide to Data Protection Act 2017 for Data Controllers (the **Guidance**)[1] published by the Cayman Ombudsman.

2 Who does the DPA apply to?

2.1 Key provision

The DPA applies[2] to a data controller in respect of any personal data only if:

(a) the data controller is established in the Cayman Islands[3] and the personal data are processed in the context of that establishment; or

(b) the data controller is not established in the Cayman Islands but the personal data are processed in the Cayman Islands otherwise than for the purposes of transit of data through the Cayman Islands (in which case the data controller shall nominate a local representative within the Cayman Islands, who shall be the data controller for all purposes within the Cayman Islands, including bearing all obligations under the DPA).

2.2 Data controllers and data processors– who are they?

The term **data controller** means 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 and includes a local representative. This definition largely reflects the definition of *controller* under the European Union's General Data Protection Regulation (**GDPR**)[4]. A data controller can be any person; which definition includes any individual, corporation, club, society, association, public authority or other body.

By contrast, a **data processor** is any person who processes data on behalf of a data controller. The data processor is a separate person from the data controller and does not include an employee of the data controller. Data processors must only act on the documented instructions of a data controller, which forms the basis of the data processor's engagement. If a data processor processes personal data outside the instructions provided by the relevant data controller, the data processor will become a data controller in its own right and will bear the obligations of a data controller under the DPA. In addition, data processors that breach their contractual obligations may be liable for damages. The Guidance contains some useful checklists relating to contracts between data controllers and data processors[5].

Subject to certain exemptions (see section 4 below), data controllers are required to:

(a) comply with the data protection principles (see section 5.1 below) applicable to the personal data that the data controller processes; or

(b) where personal data is processed on a data controller's behalf, ensure that the data protection principles are complied with in relation to the processing of that data[6].

---

1 See https://ombudsman.ky/data-protection-organisation/introduction.
2 Section 6(1), DPA.
3 Section 6(3) of the DPA states that each of the following is to be treated as "established in the Cayman Islands" :
- an individual who is ordinarily resident in the Cayman Islands;
- a body incorporated or registered as a foreign company under Cayman Islands law;
- a partnership or other unincorporated association formed under Cayman Islands law; or
- any other person that maintains in the Cayman Islands:
  - an office, branch or agency though which the person carries on any activity; or
  - a regular practice.

4 Article 4, paragraph (7), General Data Protection Regulation, Regulation (EU) 2016/679.
5 Guidance, pages 200-204.
6 Section 5(4), DPA.

2.3 Personal data

The term **personal data** means data relating to a living individual who can be identified and includes data such as:

- an individual's location data, online identifier or one or more factors specific to the identity of the living individual[7];
- an expression of opinion about the living individual; or
- any indication of the intentions of the data controller or any other person in respect of the living individual.

To be personal data, information must 'relate to' the identifiable individual. This requirement in effect introduces a further contextual assessment of the data besides the question of identifiability[8].

3 What rights are protected by the DPA?

Rather than setting out a list of obligations imposed on data controllers in their processing of personal data, the DPA sets out certain fundamental rights regarding personal data and the role of data controllers within the context of the protection afforded to those rights. These rights are set out in Part 2 of the DPA and are summarised below.

3.1 Right to be informed[9]

Individuals have the right to be informed by data controllers about the collection and use of their personal data. This is a key transparency requirement under the DPA.

In practice, a data controller must provide individuals with information including (a) who the data controller is[10] and (b) the purpose(s) for processing their personal data[11]. This information is typically communicated via a privacy notice. The Guidance contains useful information and checklists regarding the right to be informed and information which should be included in privacy notices[12]. The Guidance also provides some further 'best practice' examples of information that should be provided[13], such as the legal basis and legitimate interest of the processing, or the source and categories of the data being processed.

3.2 Right of access[14]

A person is entitled to request access to their own personal data, along with other supplementary information regarding their personal data from a data controller.

A data controller must generally comply with such a request within 30 days[15] if it has received a request in writing (a **subject access request**). The Regulations state that no fee may be charged for dealing with a subject access request, except in exceptional circumstances[16].

---

7 eg, information relating to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual.
8 Guidance page 27.
9 Section 8, DPA.
10 Guidance page 118
11 *ibid*
12 Guidance, pages 118-126.
13 Guidance, page 121
14 Section 8, DPA.
15 Where:
(a) a large amount of data is requested or is required to be searched and meeting the deadline would unreasonably interfere with the data controller's operations;
(b) more time is required to consult with third parties or other data controllers before the data controller is able to decide whether or not to give the data subject access to the requested data; or
(c) the data subject consents,
the data controller can extend the time for responding by a further 30 days or, with the permission of the Ombudsman, the period for responding can be extended for a longer period beyond 30 days. Any extension must be accompanied with an explanation to the data subject of the reason for the extension and details of when a final response will be given (Regulation 4).
16 ie, where the request from a data subject is determined to be manifestly unfounded or excessive because it is repetitive, fraudulent or would divert the resources of the data controller unreasonably.

The data subject is entitled to a copy of their personal data and any information available to the data controller as to the source of those personal data[17].

The additional information which a data subject is entitled to have access to is as follows:

(a) confirmation that their personal data is being processed by or on behalf of that data controller; and

(b) if so, a description of:

  (i) the personal data;

  (ii) the purposes for which the data are being, or are to be, processed;

  (iii) the recipients or classes of recipients to whom the data are or may be disclosed;

  (iv) any countries or territories outside the Cayman Islands to which the data controller transfers, or intends or wishes to transfer, the data (whether directly or indirectly);

  (v) general measures to be taken to comply with the seventh data protection principle (see section 5.1 below);

  (vi) any information available as to the source of the personal data;

  (vii) the reasons for any automated decision making in relation to the individual, including the data subject's performance at work, creditworthiness, reliability or conduct;

  (viii) the right to make a complaint to the Ombudsman under the DPA[18]; and

  (ix) such other information as the Commissioner may require the data controller to provide.

If a data controller cannot comply with a request made under section 8 of the DPA without disclosing personal data relating to a second data subject, the data controller is not obliged to comply with the request unless either the second data subject has consented, or it is reasonable in all the circumstances to comply without consent from the second data subject.

Section 9 of the DPA also places some limitations on the obligation of a data controller to comply with subject access requests made under section 8, including that a data controller is not required to comply with repeated requests from a single data subject unless the interval between requests is reasonable[19].

3.3 Right to stop/restrict processing[20]

A data subject is entitled at any time, by written notice to the relevant data controller, to require that processing of that subject's personal data stop, or not begin, or cease for a specified purpose or in a specified way.

This is not an absolute right and does not apply in certain circumstances (the main exceptions are set out below)[21]. If a data controller receives a notice under section 10(1) of the DPA, it must, as soon as possible and within 21 days in any case, comply with the request unless:

(a) 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;

(b) the processing is necessary for compliance with any legal obligation[22] to which the data controller is subject, other than an obligation imposed by contract;

(c) the processing is necessary in order to protect the vital interests of the data subject; or

(d) where the data controller has applied to the Ombudsman within 21 days of the date of the request by the data subject and has received approval from the Ombudsman to not comply with the data subject's request.

---

17 Section 8(2)(a) and (b)
18 Guidance, page 121
19 Section 9(3), DPA.
20 Section 10, DPA.
21 Guidance, page 148.
22 Including both common law and statutory obligations.

The data controller must inform the data subject of the reason(s) for non-compliance with a notice.

3.4 Right to stop direct marketing[23]

A data subject is entitled at any time, by written notice to the relevant data controller, to require the data controller to stop or not to begin processing their personal data for the purposes of direct marketing.

The Guidance states that this right is absolute, so there are no exemptions or grounds for refusal[24].

3.5 Rights in relation to automated decision-making[25]

A data subject is entitled at any time, by written notice to the relevant data controller, to require the data controller to require that decisions taken by or on behalf of the data controller which significantly affect the data subject are not based solely on automated processing of the data subject's personal data.

The Guidance[26] clarifies that for something to be solely automated, there must be no human involvement in the decision-making process. A decision with a mere token human involvement, such as where a human simply takes over the automated decision without any substantive appraisal, will be deemed to be automated for the purposes of the DPA.

If a data controller receives a notice requiring the cessation of automated decision-making, it must, within 21 days of receipt of the notice, provide the data subject with written notice of the steps it will take to comply with the request.

In addition, even where a data controller has not received a notice in relation to automated decision-making, but a decision that significantly affects a data subject is based solely on automated processing:

(a) the data controller must, as soon as reasonably practicable, notify the data subject that the decision was taken on that basis; and

(b) the data subject is entitled, within 21 days of receiving notification from the data controller and by notice in writing, to require the data controller to reconsider the decision or to take a new decision otherwise than on that basis.

Again, the rights in relation to automated decision-making are not absolute and will not apply to decisions:

(i) A. taken in the course of steps taken:

i. for the purposes of considering whether to enter into a contract with the data subject,
ii. with a view to entering into such a contract; or
iii. in the course of performing such a contract; or

B. authorised or required by statute; and

(ii) and:

A. the effect of the decision is to grant a request of the data subject; or
B. steps have been taken to safeguard the legitimate interests[27] of the data subject, including by allowing the data subject to make representations.

---

23 Section 11, DPA.
24 Guidance, page 154.
25 Section 12, DPA.
26 Guidance, pages 160-161.
27 Legitimate interests is the most flexible legal basis for processing, but you cannot assume it will always be the most appropriate. For more information on legitimate interests, see pages 107-109 of the Guidance.

3.6 Right to rectification[28]

The fourth data protection principle (the data accuracy principle – see section 5.1 below) requires data controllers to ensure that personal data is accurate and, where necessary, up to date. This, therefore, provides data subjects with an indirect right to have inaccurate personal data rectified or, insofar as it is incomplete, completed[29]. Accordingly, data controllers who receive a rectification request should correct inaccurate data, or update outdated data, without undue delay.

3.7 Right to seek compensation[30]

Where an individual suffers damage due to a data controller's contravention of the DPA, that person has a cause of action for compensation.

3.8 Right to complain[31]

An individual has the right to complain to the Ombudsman about any perceived violation of the DPA, and the Ombudsman may then investigate matters. A complaint has to relate to personal data processing that has not been or is not being carried out in compliance with the DPA, or anything done pursuant to the DPA.

4 Exemptions

Part 4 of the DPA[32] provides for certain situations in which the processing of personal data will be exempted from one or more of the data protection principles and/or certain provisions of the DPA itself[33]. The main exemptions are briefly described below.

4.1 National security

Meaning

Where required to safeguard national security[34].

Exempted from

All the data protection principles; and Part 2 (rights of individuals), Part 3 (personal data breaches – see section 6.3 below) and Part 6 (enforcement) of the DPA.

4.2 Crime, government fees and duties[35]

Meaning

The processing of personal data for the purposes of the prevention, detection or investigation of crime; the apprehension or prosecution of persons who are suspected to have committed an offence anywhere; the assessment or collection of any fees or duty, or of any imposition of a similar nature, in the Cayman Islands.

Exempted from

The first data protection principle (but compliance with the conditions in schedules 2 and 3 is required); the second data protection principle (purpose limitation); the third data protection principle (data minimization); section 8 (the access right); section 10 (the right to stop or restrict processing); and section 14 (the right to rectification)[36].

---

28 See pages 141-147 of the Guidance for more information.
29 And a direct right to complaint to Ombudsman if this is not done, see section 14, DPA
30 Section 13, DPA.
31 Section 43, DPA.
32 Sections 17 – 31, DPA.
33 See page 174 – 199 of the Guidance for more information.
34 Section 18, DPA. The Governor of the Cayman Islands may issue a certificate as sufficient evidence of that fact.
35 Section 19, DPA.
36 Section 19, DPA.

Where the processing is for discharging functions under any Cayman Islands law, where that data consists of information obtained for such a purpose from a person who had possession of it for any of the purposes referred to at the above meaning, processing is exempt from the first data protection principle (but compliance with the conditions in schedules 2 and 3 is required); and section 8.

4.3 Health, education or social work[37]

Meaning

(a) The health exemption applies to personal data, the release of which could reasonably cause mental or physical harm to the data subject or any other person.

(b) The education exemption applies to an educational record if its disclosure to the data subject would be likely to cause serious harm to the physical or mental health or condition of that individual or any other person.

(c) The social work exemption potentially applies to a wide range of personal data processing regarding social work (as set out in the guidance[38]) where the application of the subject information provisions[39] would be likely to prejudice the carrying out of social work. It also applies to personal data processed by a court as evidence in proceedings relating to families or children.

Exempted from

The health and social work exemptions relate to personal data which is exempt from the subject information provisions, i.e. the first data protection principle (but compliance with the conditions in schedules 2 and 3 is required); and section 8. The education exemption relates to section 8 only.

The Regulations[40] require that a data controller who is not a health professional must consult an appropriate health professional before refusing a request for information on the health exemption basis.

Regulation 9 includes further details of the social work exemption, detailing where the provision of such information would be likely to prejudice the carrying out of social work by reason of the fact that serious harm to the physical or mental health or condition of the data subject or any other person would be likely[41].

4.4 Monitoring, inspection or regulatory function[42]

Meaning

Personal data which is to be processed for the purposes of any monitoring, inspection or regulatory function connected with the exercise of a public function[43] in cases of:

(a) public safety,

(b) the prevention, investigation and prosecution of criminal offences or of ethics breaches for regulated professions; or

(c) an important economic or financial interest of the Cayman Islands[44],

Exempted from

The subject information provisions to the extent that the application of those provisions would be likely to prejudice the proper discharge of the function.

---

37 Section 20, DPA and Regulations 7 - 9.
38 Guidance, page 182
39 Per section 2, DPA, "*subject information provisions*" means - *(a) the first data protection principle to the extent to which it requires compliance with paragraph 2 of Part 2 of Schedule 1; and (b) section 8; and "third party", in relation to personal data, means any person other than - (a) the data subject; (b) the data controller; or (c) any data processor or other person authorized to process data for the data controller or data processor.*
40 Regulation 7(2).
41 Regulation 9(1).
42 Section 21, DPA.
43 For more on the meaning of *public function*, see page 105 of the Guidance.
44 Including compliance with international tax treaties.

4.5 Journalism, literature or art[45]

Meaning

Personal data to be processed only for special purposes (ie, journalistic, artistic and literary purposes) where the processing is undertaken with a view to the publication by any person of journalistic, literary or artistic material; the data controller reasonably believes the publication would be in the public interest; and the data controller reasonably believes that compliance with relevant provision of the DPA is incompatible with the special purposes.

Exempted from

The data protection principles (other than the seventh data protection principle) and Section 10.

4.6 Research, history or statistics[46]

Meaning

Personal data processed for statistical purposes or for the purposes of historical or scientific research may be exempted.

Exempted from

The first data protection principle to the extent that it requires compliance with paragraph 2(b) of Part 2 of Schedule 1 (notification of the purpose for the processing).

Personal data processed only for scientific research purpose is exempt from section 8 of the DPA (the right to access).

Personal data processed for historical, statistical or scientific purposes is exempt from the fifth data protection principle (storage limitation) to the extent that compliance would be likely to prejudice those purposes.

4.7 Corporate finance[47]

Meaning

Where personal data is to be processed for the purposes of or in connection with a corporate finance service[48] provided by a relevant person[49], the data may be exempted from the subject information provisions to the extent that:

(a) the application of those provisions could affect the price of any instrument[50] already in existence, or that is to be or may be created;

(b) the data controller reasonably believes that the application of those provisions could affect the price of any such instrument; or

(c) the exemption is required for the purposes of safeguarding an important economic or financial interest of the Cayman Islands.

---

45 Section 22, DPA.

46 Section 23, DPA.

47 Section 28, DPA.

48 Section 28(3), DPA. This term means a service consisting of:
(a) underwriting in respect of issues of, or the placing of issues of, any instrument;
(b) advice to undertakings on capital structure, industrial strategy and related matters and advice and service relating to mergers and the purchase of undertakings; and
(c) services relating to such underwriting as mentioned in (a).

49 This term includes (a) a registered person within the meaning of any Cayman Islands law providing for investment business, or a person who is exempted by the relevant law from the obligation to be registered in respect of an investment business; and (b) a person who is an authorized person under any Cayman Islands law providing for investment business, or is exempt under that law for the purposes of the investment business (section 28(3), DPA).

50 Defined as meaning an instrument representing investment within the meaning of any law in the Cayman Islands (section 28(3), DPA).

Exempted from

The first data protection principle to the extent that it requires compliance with paragraph 2(b) of Part 2 of Schedule 1 and Section 8.

4.8 Other exemptions

Other exemptions available under Part 4 of the DPA include where:

(a) the personal data consists of information that the data controller is obliged by or under an enactment to make available to the public, whether or not a fee is required[51];

(b) the disclosure of personal data is required by or under an enactment, by any law or by court order[52];

(c) the data is processed by an individual for the purposes of that individual's personal, family or household affairs[53];

(d) the personal data consists of records of the intentions of the data controller in relation to any negotiations with the data subject[54];

(e) the personal data consists of information in respect of which legal professional privilege applies[55]; and

(f) the personal data consists of information relating to a trust established under the Trusts Act (2020 Revision) or a will made pursuant to the Wills Act (2020 Revision)[56].

5 The data protection principles

5.1 The data protection principles

The eight data protection principles are stated in Part 1 of Schedule 1 to the DPA and are also set out in Schedule 2 to this Guide.

Those data protection principles fall to be interpreted in accordance with Part 2 of Schedule 1 of the DPA.

5.2 Conditions for processing personal data and sensitive personal data

A data controller must identify valid grounds under the DPA (known as **legal basis**) for handling/processing personal data. Schedule 2 to the DPA sets out the conditions or legal bases on which personal data may be processed. The main legal bases are summarised below:

(a) Consent – the individual has given clear consent (as defined in Schedule 1 to this Guide);

(b) Contract – the processing is necessary for performance of a contract with the data subject;

(c) Legal obligation – the processing is necessary for compliance with a law (this does not included contractual obligations);

(d) Vital interests – the processing is necessary to protect the vital interests[57] of the data subject;

(e) Public functions – the processing is necessary to perform a public function, e.g. the administration of justice;

(f) Legitimate interests – processing is necessary for legitimate interests pursued by a data controller or a third party.

The full text of these conditions is set out in Schedule 3 to this Guide.

---

51 Section 24 DPA
52 Section 25 DPA
53 Section 26 DPA
54 Section 29 DPA
55 Section 30 DPA
56 Section 30 DPA
57 Vital interests are intended to cover only interests that are essential for someone's life. As such, this lawful basis is very limited in its scope, and generally only applies to matters of life and death. (Guidance, page 102).

The DPA also introduces the concept of sensitive personal data (as defined in Schedule 1) which, due to its nature, is afforded additional protection. Sensitive personal data may only be processed if one of the conditions or legal bases set out in Schedule 3 to the DPA has been met. These conditions have been duplicated in Schedule 4 to this Guide.

Additional information on all of these legal bases may be found in the Guidance.

6 What are the consequences of and penalties for any breach?

6.1 Cause of action for compensation[58]

A person who suffers damage due to a data controller's contravention of the DPA has a cause of action for compensation from the data controller. As noted above, where an individual suffers damage due to a contravention of the DPA by a data controller, they may complain to the Ombudsman about any perceived violation of the DPA, or seek compensation in the courts[59].

6.2 Inaccurate personal data[60]

An individual can complain to the Ombudsman about the processing of personal data that has not been or is not being carried out in compliance with the provisions of the DPA. A data controller may be ordered by the Ombudsman to rectify, block, erase or destroy any personal data which are found to be inaccurate following a compliant made under section 43 of the DPA. The order may also extend to any other personal data in respect of which the person is the data controller which contain an expression of opinion that appears to the Commissioner to be based on the inaccurate data[61].

6.3 Personal data breaches[62]

If a personal data breach occurs, the data controller must, without undue delay but no longer than 5 days after the data controller should, with the exercise of reasonable diligence, have been aware of the breach, notify the relevant data subject(s) and the Commissioner of the breach. The notification must describe:

(a) the nature of the breach;

(b) the consequences of the breach;

(c) the measures proposed or taken by the data controller to address the breach; and

(d) the measures recommended by the data controller to the relevant data subjects to mitigate the possible adverse effects of the breach.

A data controller who contravenes these requirements commits an offence and is liable on conviction to a fine of CI$100,000 (approx. USD120,000).

7 What is the relationship between the DPA and GDPR?

The eighth data protection principle states that 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 freedom of data subjects in relation to the processing of their personal data.

GDPR[63] contains a similar provision and has recognised certain third countries and territories as "adequate". The DPA was drafted with the aim of the Cayman Islands achieving adequacy status for the purposes of the GDPR, allowing personal data to be transferred between the Cayman Islands, the member states of the EU and states found by the EU to have an adequate level of protection, in an efficient and straightforward manner. It is expected that the Cayman Islands will apply for adequacy status in due course.

For more information on GDPR, please go to our GDPR and Data Protection Information Hub here.

---

58 Section 13, DPA.
59 Guidance, page 165.
60 Section 14(1), DPA.
61 Guidance, page 141
62 Section 16, DPA. For the definition of personal data breach, see Schedule 1 of this note.
63 Regulation (EU) 2016/679.

8 Data protection and international transfers

Whilst the starting position regarding international transfers of personal data is as set out in the eighth data protection principle (see section 7 above and Schedule 2 to this Guide), Schedule 4 to the DPA sets out certain transfers which are excluded from the application of that data protection principle[64]. These transfers include:

(a) where the data subject has consented to the data transfer;

(b) where the transfer is necessary for the conclusion or performance of certain contracts;

(c) where the transfer is necessary for reasons of substantial public interest, in connection with legal proceedings or to protect the vital interests of the data subject; and

(d) where the transfer is necessary for the purposes of international cooperation between intelligence or regulatory agencies to combat organized crime, terrorism or drug trafficking or to carry out other cooperative functions, provided that such disclosure is permitted or required by Cayman Islands law or court order.

Mourant Ozannes

Our team of data protection specialists can:

- provide DPA legal advice;
- assist in the review of current policies and procedures to help identify gape or areas where common problems may arise and where work is likely to be needed as a result of the DPA;
- review and draft relevant contracts and policy documents;
- review and draft privacy notices; and
- assist in litigation relating to the DPA, including complaints to the Ombudsman, claims for compensation and judicial reviews of decisions of the Ombudsman relating to the DP.

A full list of contacts specialising in the DPA can be found here.

[64] Section 5(3), DPA.

Schedule 1 - Definitions

Commissioner	means the person appointed as Ombudsman under section 3 of the Ombudsman Act, 2017 (n.b. the DPA refers to an "Information Commissioner" appointed under s.35 of the Freedom of Information Act (2020 Revision). This section was repealed by the Freedom of Information (Amendment) Act 2017; and the Freedom of Information Act (2020 Revision) and Ombudsman Act, 2017 make it clear that these functions are to be performed by the Ombudsman.)
consent	in relation to a data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which the data subject, by a statement or clear affirmative action, signifies agreement to the processing of personal data relating to the said data subject.[65]
data subject	means – (a) an identified living individual; or (b) a living individual who can be identified directly or indirectly by means reasonably likely to be used by a data controller or by any other person.
direct marketing	for the purposes of section 11 of the DPA, means the communication, by whatever means, of any advertising, marketing, promotional or similar material, that is directed to particular individuals.
personal data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or other processed.
processing	in relation to data, means obtaining, recording or holding data, or carrying out any operation or sets of operations on personal data, including – (a) organizing, adapting or altering the personal data; (b) retrieving, consulting or using the personal data; (c) disclosing the personal data by transmission, dissemination or otherwise making it available; or (d) aligning, combining, blocking, erasing or destroying the personal data.

[65] In addition, section 5(5) of the DPA provides that the provisions of Schedule 5 shall apply to any determination of consent under the DPA. Schedule 5 to the DPA sets out four conditions of consent, which are summarized below:

1. The data controller shall bear the burden of proving a data subject's consent to processing of personal data;
2. If consent is in the form of a written declaration which also concerns another matter, the requirement to give consent shall be presented in a manner which is distinguishable from the other matter.
3. Consent can be withdrawn at any time by the data subject.
4. Where there is a significant imbalance between the data controller and the data subject, consent shall not provide a legal basis for processing.

sensitive personal data	means, in relation to a data subject, personal data consisting of – (a) the racial or ethnic origin of the data subject; (b) the political opinions of the data subject; (c) the data subject's religious beliefs or other beliefs of a similar nature; (d) whether the data subject is a member of a trade union; (e) genetic data of the data subject; (f) the data subject's physical or mental health or condition; (g) medical data; (h) the data subject's sex life; (i) the data subject's commission, or alleged commission, of an offence; or (j) any proceedings for any offence committed, or alleged to have been committed, by the data subject, the disposal of any such proceedings or any sentence of a court in the Cayman Islands or elsewhere.
subject information provisions	means the first data protection principle, to the extent to which it requires compliance with Paragraph 2 of Part 2 of Schedule 1 to the DPA[66] and section 8 (fundamental rights of access to personal data) of the DPA.

[66] Paragraph 2 of Part 2 of Schedule 1 to the DPA provides that, for the purposes of the first data protection principle, personal data shall not be treated as processed fairly unless the data subject has, as soon as reasonably practicable, been provided with, at a minimum, (a) the identity of the data controller and (b) the purpose for which the data are to be processed.

Schedule 2 – The data protection principles

First principle (Fair and lawful)	Personal data shall be processed fairly. In addition, personal data may be processed only if – (a) in every case, at least one of the conditions set out in paragraphs 1 to 6 of Schedule 3 is met (see paragraph 5.2 above); and (b) in the case of sensitive personal data, at least one of the conditions in paragraphs 1 to 10 of Schedule 4 is also met (see paragraph 5.2 above)[67].
Second principle (Purpose limitation)	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.
Third principle (Data minimization)	Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are collected or processed.
Fourth principle (Data accuracy)	Personal data shall be accurate and, where necessary, kept up to date.
Fifth principle (Storage limitation)	Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
Sixth principle (Respect for the individual's rights)	Personal data shall be processed in accordance with the rights of data subjects under the DPA.
Seventh principle (Security)	Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
Eighth principle (International transfers)	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.

[67] In order to legally process sensitive personal data, one must identify both a legal basis (condition) for processing in Schedule 2 as well as a basis for processing sensitive personal data in Schedule 3 of the DPA (the Guidance, page 114).

Schedule 3 – Conditions for processing personal data

1.	Consent	The data subject has given consent to the processing[68].
2.	Processing necessary for contract	The processing is necessary for – (a) the performance of a contract to which the data subject is a party; or (b) the taking of steps at the request of the data subject with a view to entering into a contract.
3.	Processing under legal obligation	The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4.	Processing to protect vital interests	The processing is necessary in order to protect the vital interests of the data subject.
5.	Processing necessary for exercise of public functions	The processing is necessary for – (a) the administration of justice; (b) the exercise of any functions conferred on any person by or under any enactment; (c) the exercise of any function of the Crown or any public authority; or (d) the exercise of any other functions of a public nature exercised in the public interest by any person.
6.	Processing for legitimate interests	The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except if the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
7.	Regulations about legitimate interests	The Cabinet may, by regulations, specify particular circumstances in which the condition set out in paragraph 6 shall, or shall not, be taken to be satisfied[69].

[68] The DPA sets a high standard for consent. For more information, see the definition of **consent** in Schedule 1 to this Guide and page 89 of the Guidance.

[69] The Regulations themselves do not address this point. See page 107 of the Guidance for more information.

Schedule 4 – Conditions for processing sensitive personal data

1.	Consent	The data subject has given consent to the processing of the personal data.
2.	Employment	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.
3.	Vital interests	The processing is necessary – (a) in order to protect the vital interests 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 (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
4.	Non-profit associations	The processing – (a) is carried out in the course of its legitimate activities by a body, or association, that is not established or conducted for profit, and exists for political, philosophical, religious or trade union purposes; (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects; (c) relates only to data subjects who are members of the body or association or have regular contact with it in connection with its purposes; and (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.
5.	Information made public by data subject	The information contained in the personal data has been made public as a result of steps taken by the data subject.
6.	Legal proceedings, etc.	The processing – (a) is necessary for the purpose of, or in connection with, any legal proceedings; (b) is necessary for the purpose of obtaining legal advice; or (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
7.	Public functions	The processing is necessary for – (a) the administration of justice; (b) the exercise of any functions conferred on any person by or under an enactment; or (c) the exercise of any functions of the Crown or any public authority.

8.	**Medical purposes**	The processing is necessary for medical purposes[70] and is undertaken by – (a) a health professional; or (b) a person who, in the circumstances, owes a duty of confidentiality equivalent to that which would arise if that person were a health professional.
9.	**Circumstances prescribed by regulations**	The personal data are processed in such circumstances prescribed by regulations.
10.	**Regulations relating to paragraph 2 or 7**	The Cabinet may by regulations – (a) exclude the application of paragraph 2 or 7 in such cases as may be specified; or (b) provide that, in such cases as may be specified, the conditions in paragraph 2 or 7 shall not be regarded as satisfied unless such further conditions, as may be specified in the regulations, are also satisfied[71].

[70] **Medical purposes** includes the purposes of preventative medicine, medical diagnosis, the provision of care and treatment and the management of healthcare services.

[71] The Regulations do not currently detail any provisions regarding paragraphs 2 or 7.