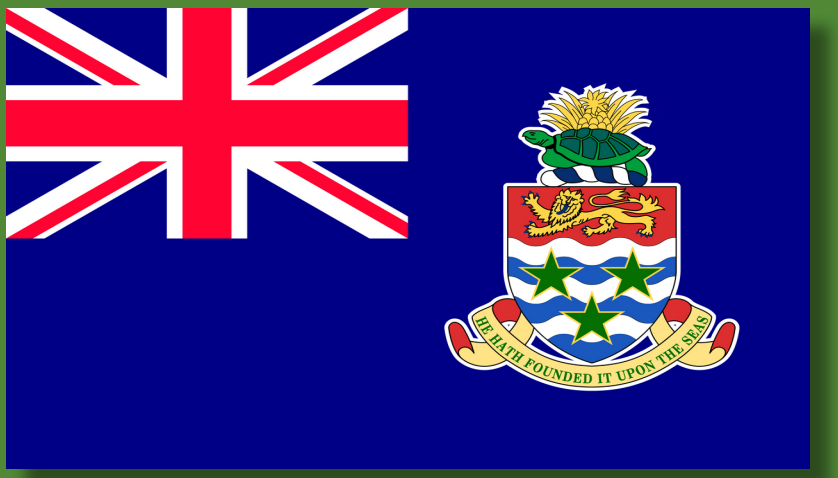


Comparing privacy laws: GDPR v. Data Protection Act

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

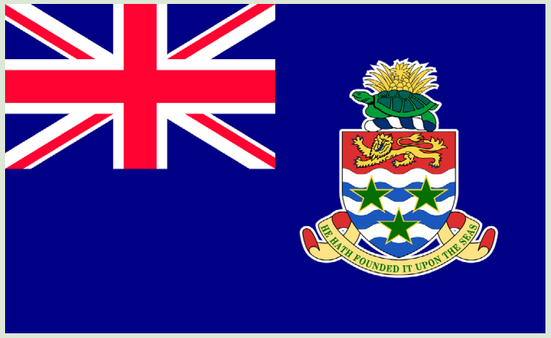
OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

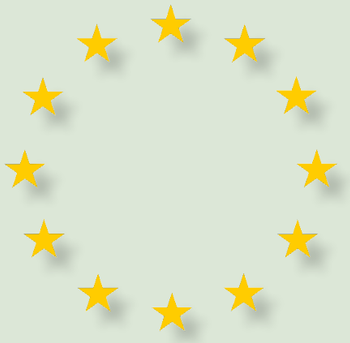
The OneTrust DataGuidance™ platform includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Cross-Border Charts which allow you to compare Act across multiple jurisdictions at a glance, a daily customised news service and expert analysis.

These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy programme.

Image production credits:
Cover/p.5/p.51: 221A / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com
Icon p.33-40: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.47-51: cnythzl / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com

Table of contents





Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') came into effect on 25 May 2018 and governs the protection of personal data in EU and EEA Member States. The Data Protection Act (2021 Revision) ('the Act') is the primary piece of data protection legislation in the Cayman Islands, which updated the Data Protection Law, 2017 (Law 33 of 2017). The Act established the Office of the Ombudsman ('the Ombudsman') and is supplemented by the Data Protection Regulations, 2018 (SL 17 of 2019) ('the Regulations').

The Act is based on eight principles, which provide a general framework for personal data protection that is similar to the GDPR. For instance, the Act sets out requirements for data subject rights, breach notifications, data transfers, and sensitive data. Indeed, the Act cites European adequacy decisions as a basis for enabling international data transfers. However, the GDPR and the Act differ in areas such as data protection officer and impact assessment obligations, and the Act combines rights to information and access.

This overview organises provisions from the GDPR and the Act into key topics and sets them alongside each other to enable analysis and comparison. Each section begins with a detailing of principal information and a general introduction, as well as a consistency rating.

Structure and overview of the Guide

This Guide provides a comparison of the two legislative frameworks on the following key provisions:

1. Scope
2. Key definitions
3. Legal basis
4. Controller and processor obligations
5. Individuals' rights
6. Enforcement

Each topic includes relevant provisions from the two legislative legal frameworks, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the Act.

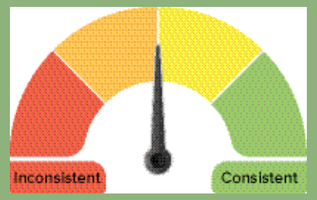
Key for giving the consistency rate

Consistent: The GDPR and the Act bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.

Fairly consistent: The GDPR and the Act bear a high degree of similarity in the rationale, core, and the scope of the provision considered, however, the details governing its application differ.

Fairly inconsistent: The GDPR and the Act bear several differences with regard to the scope and application of the provision considered, however, its rationale and core presents some similarities.

Inconsistent: The GDPR and the Act bear a high degree of difference with regard to the rationale, core, scope, and application of the provision considered.



Usage of the Guide

This Guide is general and informational in nature, and is not intended to provide, and should not be relied on as a source of, legal advice. The information and materials provided in the Guide may not be applicable in all (or any) situations and should not be Acted upon without specific legal advice based on particular circumstances.

1. Scope

Fairly consistent

1.1. Personal scope

The Act employs similar core concepts as the GDPR and refers to data controllers, data processors, and data subjects. Like the GDPR, the Act also includes public bodies within its scope and excludes deceased individuals. The GDPR and the Act differ, however, in that the latter does not refer to the nationality or place of residence of data subjects.

GDPR	Act
Data controller	
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	Section 2 of the Act: '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 referred to in Section 6(2) of the Act.
Data processor	
Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	Section 2 of the Act: 'data processor' means any person who processes personal data on behalf of a data controller but, for the avoidance of doubt, does not include an employee of the data controller.
Data subject	
Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fActors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Section 2 of the Act: '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 the data controller or by any other person.
Public bodies	
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body.	Section 2 of the Act: 'person' includes any corporation, either aggregate or sole, and any club, society, association, public authority or other body, of one or more persons.

GDPR	Act
Nationality of data subject	
Recital 14: The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.	The Act does not refer to the nationality of data subjects.
Place of residence	
See Recital 14, above.	The Act does not refer to the place of residence of data subjects.
Deceased individuals	
Recital 27: This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.	Section 2 of the Act: 'personal data' means data relating to a living individual.

1.2. Territorial scope

Fairly inconsistent

In general terms, and unlike the GDPR, the Act does not apply extraterritorially, nor does it explicitly regulate goods and services or monitoring from abroad. The Act does, however, specify that it applies to data controllers established in the Cayman Islands or that process personal data in the Cayman Islands for purposes other than the transit of such data.

GDPR	Act
Establishment in jurisdiction	
Article 3: This Regulation applies to the processing of personal data in the context of the Activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. Recital 22: Establishment implies the effective and real exercise of Activity through stable arrangements.	Section 6 of the Act: (1) The Act applies to a data controller in respect of any personal data only if (a) the data controller is established in the Islands and the personal data are processed in the context of that establishment; or (b) the data controller is not established in the Islands but the personal data are processed in the Islands otherwise than for the purposes of transit of the data through the Islands. (2) A data controller referred to in Section 6(1)(b) of the Act shall nominate, for the purposes of the Act, a local representative established in the Islands who shall, for all purposes within the Islands, be the data controller and, without limiting the generality of this provision, bear all obligations under the Act as if the representative were the data controller. (3) For the purposes of Section 6(1) and (2) of the Act, each of the following is to be treated as established in the Islands: (a) an individual who is ordinarily resident in the Islands; (b) a body incorporated or registered as a foreign company under the law of the Islands; (c) a partnership or other unincorporated association formed under the law of the Islands; or (d) any person who does not fall within paragraph (a), (b) or (c) but maintains in the Islands: (i) an office, branch or agency through which the person carries on any activity; or (ii) a regular practice.
Extraterritorial	
See Article 3, above.	See Section 6 of the Act, above.
Goods & servicies from abroad	
Recital 23: In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing Activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.	The Act does not refer to goods and services from abroad.

GDPR	Act
Monitoring from abroad	
Recital 24: The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.	The Act does not refer to monitoring from abroad.

Fairly consistent

1.3. Material scope

The Act and the GDPR provide similar definitions of personal data and data processing, as well as setting out specific requirements for special categories of, or sensitive, data. The two pieces of legislation differ, however, in terms of the general exemptions they stipulate, and in regard to automated processing, anonymised, and pseudonymised data.

GDPR	Act
Personal data/ personal information	
Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fActors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Section 2 of the Act: 'personal data' means data relating to a living individual who can be identified and includes data such as: (a) the living individual's location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the living individual; (b) an expression of opinion about the living individual; or (c) any indication of the intentions of the data controller or any other person in respect of the living individual.
Data processing	
Article 4(2): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.	Section 2 of the Act: 'processing', in relation to data, means obtaining, recording, or holding data, or carrying out any operation or set of operations on personal data, including: (a) organising, 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.
Special categories of data	
Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	Section 3 of the Act: '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;

GDPR	Act
Special categories of data (cont'd)	
	(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 Islands or elsewhere.
Anonymised data	
Recital 26: The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	The Act does not refer to anonymised data.
Pseudonymised data	
Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	The Act does not refer to pseudonymised data. However, this is addressed within the Data Protection Act (2021 Revision) Guide for Data Controllers ('the Data Controllers Guide').
Automated processing	
Article 2(1): This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.	The Act does not define automated processing. However, Section 12 of the Act provides for specific data subject rights in relation to automated decision making (see section 6.5. below).
General exemptions	
Article 2(2): This Regulation does not apply to the processing of personal data: (a) in the course of an Activity which falls outside the scope of Union law; (b) by the Member States when carrying out Activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union; or (c) by a natural person in the course of a purely personal or household Activity.	Sections 18-31 of the Act: The Act does not fully apply to the processing of personal data where it is processed for the following purposes or contexts: national security; crime, government fees and duties; health, education or social work; monitoring, inspection or regulatory function; journalism, literature or art; research, history or statistics;

GDPR	Act
General exemptions (cont'd)	
	information available to public by or under enactments; disclosures required by law or made in connection with legal proceedings; personal, family or household affairs; honours; corporate finance; negotiations; legal professional privilege and trusts; and exemptions by regulations.

2. Key definitions

2.1. Personal data

Fairly consistent

The GDPR and the Act set out similar understandings for the concepts of personal data and sensitive, or special categories of, data as well as health data. The two pieces of legislation differ in certain specific aspects, for instance the Act includes opinions within its definition of personal data and does not provide examples of what it means by online identifiers.

GDPR	Act

Personal data/ personal information

Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fActors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Section 2 of the Act: 'personal data' means data relating to a living individual who can be identified and includes data such as -
(2) the living individual's location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the living individual;
(3) an expression of opinion about the living individual; or
(4) any indication of the intentions of the data controller or any other person in respect of the living individual.

Special categories of data

Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Section 3 of the Act: '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 Islands or elsewhere.

GDPR	Act

Online identifiers

Recital 30: Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

Online identifiers are included in the definition of personal data, see Section 2 of the Act above. However, no further examples are provided.

Other

Not applicable.

Section 2 of the Act: 'health record' means a record that:
(a) consists of information relating to the physical health, mental health or condition of a data subject; and
(b) has been made by or on behalf of a health professional in connection with the care of that data subject.

2.2. Pseudonymisation

Unlike the GDPR, the Act does not directly refer to anonymisation and pseudonymisation, although there are provisions that are relevant.

GDPR	Act

Anonymisation

Recital 26: 'anonymous information' is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

The Act does not define anonymisation. In relation to exempting research purposes from certain requirements, Section 23(6)(c) of the Act refers to an obligation that 'the results of the research or any resulting statistics are not made available in a form that identifies one or more of the data subjects'.

Pseudonymisation

Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

The Act does not define pseudonymisation. In relation to data subjects' rights to information and access, Section 8(9) of the Act notes: 'Subsection (7) shall not be construed as excusing a data controller from communicating so much of the personal data sought in the request as can be communicated without disclosing the identity of the other data subject concerned, whether by the omission of names or other identifying particulars or otherwise'.

2.3. Controllers and processors

The Act and the GDPR provide similar definitions for data controllers and data processors, as well as requirements for agreements between these parties. However, unlike the GDPR, the Act does not address Data Protection Impact Assessments ('DPIA') or data protection officer ('DPO') appointments.

GDPR	Act

Data controller

Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Section 2 of the Act: '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 referred to in Section 6(2) of the Act.
Section 6(2) of the Act: A data controller referred to in Section 6(1)(b) of the Act shall nominate, for the purposes of the Act, a local representative established in the Islands who shall, for all purposes within the Islands, be the data controller and, without limiting the generality of this provision, bear all obligations under the Act as if the representative were the data controller.

Data processor

Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Section 2 of the Act: 'data processor' means any person who processes personal data on behalf of a data controller but, for the avoidance of doubt, does not include an employee of the data controller.

Controller and processor contracts

Article 28(3): Processing by a processor shall be governed by a contrAct or other legal Act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. [Article 28 goes on to stipulate necessary information to be included in such a contract.]

Seventh Principle under Schedule 1, Part 2(3) of the Act: If processing of personal data is carried out by a data processor on behalf of a data controller, the data controller shall not be regarded as complying with the seventh principle unless the processing is carried out under a contract (a) that is made or evidenced in writing; (b) under which the data processor is to act only on instructions from the data controller; and (c) that requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.
Seventh Principle under Schedule 1, Part 1 of the Act: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

GDPR	Act
Data Protection Impact Assessment ('DPIA')	
DPIA is not specifically defined, however Article 35 sets out requirements for DPIAs (see section 5.3. for further information).	The Act does not address DPIAs.
Data Protection Officer ('DPO')	
DPO is not specifically defined, however Article 37 sets out requirements related to DPOs (see section 5.4. for further information).	The Act does not provide requirements for DPOs.

2.4. Children

Unlike the GDPR, the Act does not provide additional requirements for children's data. The Regulations provide an age threshold under which a person is considered a child, and set out further provisions that primarily consider children's data within the education sector.

GDPR	Act
Children's definition	
The GDPR does not specifically define 'child'. However, Article 8(1) provides: Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.	Section 2 of the Regulations: 'child' means a person under the age of 18 years.
Consent for processing children's data	
Article 8(2): The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.	The Act does not address consent for processing children's data.
Privacy notice (children)	
Recital 58: Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.	The Act does not address notifications in relation to children's data.

2.5. Research

Fairly consistent

Like the GDPR, the Act provides exemptions for processing for scientific or historical research purposes. However, the Act does not establish requirements for appropriate safeguards in the manner of the GDPR, although it does set out certain obligations in order to be exempted from data subject rights when processing for research purposes.

GDPR	Act

Scientific/ historical research definition

Recital 159: Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.
Recital 160: Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

The Act does not define or provide examples of scientific or historical research purposes.

Compatibility with original purpose of collection

Article 5(1)(b): Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').

Section 23(4) of the Act: For the purposes of the second data protection principle, the further processing of personal data for the purpose of research, history or statistics in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which they were obtained.
Section 23(7) of the Act: Personal data processed for historical, statistical or scientific purposes in compliance with the relevant conditions are exempt from the fifth data protection principle to the extent to which compliance would be likely to prejudice those purposes.
Fifth Principle under Schedule 1, Part 1 of the Act: Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

Appropriate safeguards

Article 89(1): Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical

The Act does not establish requirements for appropriate safeguards in relation to processing for scientific or historical research purposes.

GDPR	Act

Appropriate safeguards

and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner.

Data subject rights (research)

Under Article 17(3), the right to erasure may not apply in cases of scientific or historical research. Article 21(6), however, provides that data subjects may exercise the right to object to data processing for scientific or historical research purposes. In addition, Article 89 provides that Member States may derogate from the GDPR in regard to data subject rights and data processing for research purposes.

Section 23 of the Act: (1) In this Section, 'relevant conditions' means: (a) the condition that the personal data are not processed to support a measure or decision with respect to a particular data subject; and (b) the condition that the personal data are not processed in such a way that substantial damage or substantial distress is likely to be caused to any data subject.
Section 23(5) of the Act: Personal data processed solely for the purposes of scientific research or kept in a form that identifies a data subject for a period which does not exceed the period necessary for the sole purpose of creating statistics are exempt from Section 8 of the Act.
Section 23(6) of the Act: Section 23(5) of. theAct applies if:
(a) the data are processed in compliance with the relevant conditions;
(b) there is no risk of breaching the rights and freedoms of the data subject; and
(c) the results of the research or any resulting statistics are not made available in a form that identifies one or more of the data subjects.
[Note: Part 2 of the Act provides certain data subject rights].

3. Legal basis

Fairly consistent

The Act sets out very similar grounds for the processing of personal data to the GDPR, as well as comparable additional requirements for the processing of sensitive data. Moreover, the Act has provisions defining conditions for consent, and addresses matters such as processing for journalistic/artistic purposes.

GDPR	Act

Legal grounds

Article 6(1): Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contrAct to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contrAct;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Schedule 2 of the Act: Conditions for processing of personal data:

1. The data subject has given consent to the processing.

2. 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. 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. The processing is necessary in order to protect the vital interests of the data subject.

5. 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 functions 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. 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. 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.

GDPR	Act

Sensitive data (legal basis)

There are specific requirements for processing special categories of data, see Article 9 of the GDPR for further information.

There are specific requirements for processing special categories of data, see Schedule 3 of the Act for further information.

Conditions for consent

Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

Article 4: (11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative Action, signifies agreement to the processing of personal data relating to him or her.

Schedule 5 of the Act - Conditions of consent:
1. The data controller shall bear the burden of proving the data subject's consent to the processing of the data subject's personal data for the specified purposes.
2. If the data subject's consent is to be given in the form of a written declaration which also concerns another matter, the requirement to give consent shall be presented in an appearance that is distinguishable from the other matter.
3. The data subject shall have the right to withdraw consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
4. Where there is a significant imbalance between the position of the data subject and the data controller, consent shall not provide a legal basis for the processing.

Journalism/artistic purposes

Article 85(1): Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

Section 4 of the Act: In this Act, 'special purposes' means any one or more of the following: (a) the purposes of journalism; (b) artistic purposes; and (c) literary purposes.
Section 22(1) of the Act: Personal data which are processed only for the special purposes are exempt from any provision to which this Section relates if:
(a) the processing is undertaken with a view to the publication by a person of any journalistic, literary or artistic material;
(b) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest; and
(c) the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes.
Section 22(2) of the Act: This Section relates to the following provisions: (a) the data protection principles except the seventh data protection principle; and (b) Section 10 of the Act.
[Note: Section 10 of the Act establishes the data subject's right to restrict processing].

4. Controller and processor obligations

4.1. Data transfers

The Act provides for a similar notion of adequate protection as the GDPR and, although the Act does not outline mechanisms for data transfers such as binding corporate rules, the Act stipulates a limited number of mechanisms for data transfers such as transfers relating to the performance of contract.

GDPR	Act

Adequate protection

Article 45(1): A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

Eight Principle under Schedule 1, Part 1 of the Act: 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.
Point 4 of the Eighth Principle under Schedule 1, Part 2 of the Act: For the purposes of the eighth principle, an adequate level of protection is one that is adequate in all the circumstances of the case, having regard to, among other things, to:
(a) the nature of the personal data;
(b) the country or territory of origin of the information contained in the data;
(c) the country or territory of final destination of that information;
(d) the purposes for which and period during which the personal data are intended to be processed;
(e) the law in force in the country or territory in question;
(f) the international obligations of that country or territory;
(g) any relevant codes of conduct or other rules that are enforceable in that country or territory, whether generally or by arrangement in particular cases; and
(h) any security measures taken in respect of the data in that country or territory.
Point 6 of the Eighth Principle under Schedule 1, Part 2 of the Act: (1) If in any proceedings under the Act a question arises as to whether the requirement of the eighth principle as to an adequate level of protection is met in relation to the transfer of any personal data to a country or territory outside the Islands which is a member state of the EU or with respect to which a EU finding has been made in relation to transfers of the kind in question, that question shall be determined in accordance with that finding. (2) In this paragraph 'European

GDPR	Act

Adequate protection (cont'd)

Union finding' means a finding of the European Commission, under the procedure provided for in Article 93 of the GDPR or such other provision or instrument as may for the time being be in force on the protection of data subjects with regard to the processing of personal data and on the free movement of such data, that a country or territory outside the European Economic Area does, or does not, ensure an adequate level of protection within the meaning of Article 45 of the GDPR or such other provision or instrument as may for the time being be in force for that purpose.

Other mechanisms for data transfers

Article 46(1): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.
(2) The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:
(a) a legally binding and enforceable instrument between public authorities or bodies;
(b) binding corporate rules in accordance with Article 47;
(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable

Schedule 4 of the Act: Transfers to which the eighth principle does not apply:
1. The data subject has consented to the transfer.
2. The transfer is necessary for: (a) the performance of a contract between the data subject and the data controller; or (b) 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.
3. The transfer is necessary for: (a) 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 (b) the performance of such a contract.
4. The transfer is necessary for reasons of substantial public interest.
5. The transfer: (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.
6. The transfer is necessary in order to protect the vital interests of the data subject.
7. 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.
8. The transfer is made on terms of a kind approved by the Ombudsman as ensuring adequate safeguards for the rights and freedoms of data subjects.
9. The transfer has been authorised by the Ombudsman

GDPR	Act
Other mechanisms for data transfers (cont'd)	
commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights. (3) Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by: (a) contrActual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.	as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects. 10. The transfer is required under international cooperation arrangements between intelligence agencies or between regulatory agencies to combat organised crime, terrorism or drug trafficking or to carry out other cooperative functions. 11. The Cabinet may, by regulations, specify in broad, non-exhaustive terms: (a) circumstances in which a transfer shall be taken for the purposes paragraph 4 to be necessary for reasons of substantial public interest; and (b) circumstances in which a transfer not required by or under an enactment shall not be taken, for the purposes of paragraph 4, to be necessary for reasons of substantial public interest.
Data localisation	
Not applicable.	Not applicable.

4.2. Data processing records

While the GDPR requires both data controllers and data processors to maintain data processing records, the Act does not specify equivalent obligations for either. However, the Act does set out general provisions for providing information to the Ombudsman, as well as the format of such information.

GDPR	Act
Data controller obligation	
Article 30(1): Each controller and, where applicable, the controller's representative, shall maintain a record of processing Activities under its responsibility. That record shall contain all of the following information: (a) the name and contAct details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (f) where possible, the envisaged time limits for erasure of the different categories of data; and (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).	The Act does not specify obligations for data controllers to maintain data processing records.

GDPR	Act

Data processor obligation

Article 30(2): Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing Activities carried out on behalf of a controller, containing:
(a) the name and contAct details of the processor or processors and of each controller on behalf of which the processor is Acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
(b) the categories of processing carried out on behalf of each controller;
(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; and
(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

The Act does not specify obligations for data processors to maintain data processing records.

Records format

Article 30(3): The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

Section 60(2) of the Act: A notice or other document which is required or authorised under the Act to be given to the Ombudsman may be given by electronic or other means on the condition that the Ombudsman is able to obtain or recreate the notice or document in intelligible form.

Required to make available

Article 30(4): The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

Section 49(1) of the Act: Except as provided in the Act, no enactment or law prohibiting or restricting the disclosure of information shall preclude a person from furnishing the Ombudsman with any information required for the discharge of the Ombudsman's functions under the Act.

Exemptions

Article 30(5): The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

The Act does not provide specific exemptions from data processing record requirements.

GDPR	Act

General Data Processing Notification ('DPN')

Not applicable.

Section 15 of the Act: The Cabinet may, after consultation with the Ombudsman and such other persons that the Cabinet may consider appropriate, make regulations prescribing the types of processing that require the prior approval of the Ombudsman, being processing that is considered particularly likely to (a) cause substantial damage or substantial distress to data subjects; or (b) otherwise significantly prejudice the rights and freedoms of data subjects.

[Note: Such regulations have yet to be introduced.]

4.3. Data protection impact assessment

The Act does not provide requirements on DPIAs. However, the Ombudsman has provided non-binding guidance on the Act, which suggests that privacy impact assessments are best practice (see the Data Controllers Guide).

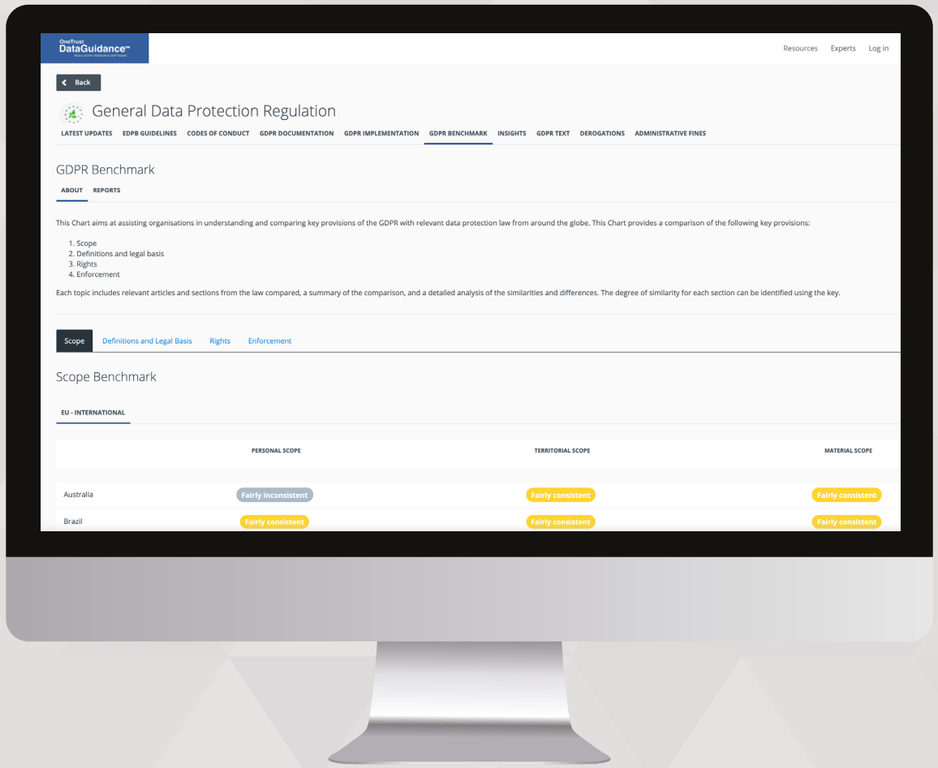
GDPR	Act
When is a DPIA required	
Article 35(1): Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. [...] (3) A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale.	The Act does not provide requirements for DPIAs.
DPIA content requirements	
Article 35(7): The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including	The Act does not provide requirements for DPIAs.

GDPR	Act
DPIA content requirements	
safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.	
Consultation with authority	
Article 36(1): The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. [Article 36 goes on to detail requirements related to such prior consultation].	The Act does not provide requirements for DPIAs.

Global Regulatory Research Software

40 In-House Legal Researchers, 500 Lawyers Across 300 Jurisdictions

Monitor regulatory developments, mitigate risk, and achieve global compliance



Build a global privacy program by comparing key legal frameworks against the GDPR

CCPA | Russia | Thailand | Brazil | Japan | China
and 20+ other global laws & frameworks

Understand and compare key provisions of the GDPR with relevant data protection laws from around the globe

The GDPR Benchmarking tool provides comparison of the various pieces of legislation on the following key provisions

- Scope
- Rights
- Definitions and legal basis
- Enforcement

- Employ topic specific guidance to develop your compliance activities
- Monitor news and access written opinion pieces on the most recent developments

OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

Start your free trial at
www.dataguidance.com

4.4. Data protection officer appointment

Unlike the GDPR, the Act does not provide requirements for data protection officers.

GDPR	Act
DPO tasks	
Article 39(1): The data protection officer shall have at least the following tasks: (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; (d) to cooperate with the supervisory authority; and (e) to Act as the contAct point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.	The Act does not provide requirements for DPOs.
When is a DPO required	
Article 37(1): The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts Acting in their judicial capacity; (b) the core Activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or	The Act does not provide requirements for DPOs.

GDPR	Act
When is a DPO required (cont'd)	
(c) the core Activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.	
Group appointments	
Article 37(2): A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.	The Act does not provide requirements for DPOs.
Notification of DPO	
Article 37(7): The controller or the processor shall publish the contAct details of the data protection officer and communicate them to the supervisory authority.	The Act does not provide requirements for DPOs.
Qualifications	
Article 37(5): The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and prActices and the ability to fulfil the tasks referred to in Article 39.	The Act does not provide requirements for DPOs.

4.5. Data security and data breaches

While the Act provides that breach notifications be made to the Ombudsman and a requirement to have security measures in place, these provisions are significantly less detailed than the GDPR.

GDPR	Act

Security measures defined

Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Seventh Principle under Schedule 1, Part 1 of the Act: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Data breach notification to authority

Article 33(1): In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Section 16(1) of the Act: In the case of a personal data breach, the data controller shall, without undue delay, but no longer than five days after the data controller should, with the exercise of reasonable diligence, have been aware of that breach, notify the data subject of the data in question and the Ombudsman of that personal data breach, describing:
(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

GDPR	Act

Data breach notification to authority

(d) the measures recommended by the data controller to the data subject of the personal data in question to mitigate the possible adverse effects of the breach.

Timeframe for breach notification

See Article 33(1) above.

See Section 16(1) of the Act above.

Notifying data subjects of data breach

Article 34(1): When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

See Section 16(1) of the Act above.

Data processor notification of data breach

Article 33(2): The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

The Act does not provide for data processor notification requirements for data breaches. [Note: The Ombudsman has issued the Data Controllers Guide which recommends data processor notifications of data breaches.]

Exceptions

Article 34(3): The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Section 18 of the Act: (1) Personal data are exempt from any of the provisions of (a) the data protection principles; and (b) Parts 2, 3, and 6, if the exemption from any or all of the provisions is required for the purpose of safeguarding national security.
(2) The Governor may, for the purpose mentioned in Subsection (1), issue a certificate with respect to any personal data exempting that data from all or any of the provisions referred to in that Subsection and that certificate shall be sufficient evidence of that fact.
Section 26 of the Act: Personal data processed by an individual only for the purposes of that individual's personal, family or household affairs are exempt from the data protection principles and Parts 2 and 3 of the Act.

4.6. Accountability

Unlike the GDPR, the Act does not explicitly address a concept of accountability or define the liabilities of data controllers and processors. The Act generally provides that 'persons' are liable for offences without distinguishing between controllers and processors for liability.

GDPR	Act
Principle of accountability	
Article 5(2): The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability'). [Paragraph 1 details principles of: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality.]	The Act does not directly address a principle of accountability.
Liability of data controllers and data processors	
Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has Acted outside or contrary to lawful instructions of the controller.	The Act does not specify the liabilities of 'persons' and does not clarify a difference in liability between data controllers and processors.

5. Rights

5.1. Right to erasure

Although the Act stipulates a right for processing to be ceased, it is significantly more limited in detail and scope than that provided for under the GDPR. The Act also does not clarify matters such as fees or response timeframes.

GDPR	Act
Grounds for erasure	
Article 17(1): The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).	Section 14(1) of the Act: If the Ombudsman is satisfied on a complaint made under Section 43 of the Act that personal data are inaccurate, the Ombudsman may order the data controller to rectify, block, erase or destroy (a) those data; and (b) any other personal data in respect of which the person is the data controller and that contain an expression of opinion that appears to the Ombudsman to be based on the inaccurate data.
Inform data subject of right	
Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.	The Act does not address the requirement to inform data subjects of the right to erasure in general terms.

GDPR	Act

Inform data subject of right

Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Fees

Article 12(5): Information provided under Articles 13 and 14 and any communication and any Actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive charActer, the controller may either:
(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the Action requested; or
(b) refuse to Act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive charActer of the request.

The Act does not address the fees for a response to a request to erase data.

GDPR	Act

Response timeframe

Article 12(3): The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

The Act does not address the timeframe for a response.

Format of response

Article 12(1): The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The Act does not address the format of a response to a request to erase data.

Publicly available data

Article 17(2): Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

Section 24 of the Act: Personal data are exempt from (a) the subject information provisions; (b) the fourth data protection principle and Section 14(1) to (3); and (c) the non-disclosure provisions, if the data consist of information that the data controller is obliged by or under any enactment to make available to the public, including by inspection, gratuitously or on payment of a fee.

Exceptions

Article 17(3): Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
(a) for exercising the right of freedom of expression and information;
(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(c) for reasons of public interest in the area of

See the general exceptions in Sections 18-30 of the Act as noted above in section 1.3.

GDPR	Act

Exceptions (cont'd)

public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
(e) for the establishment, exercise or defence of legal claims.
Article 12(5): Information provided under Articles 13 and 14 and any communication and any Actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive charActer, the controller may either:
(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the Action requested; or
(b) refuse to Act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive charActer of the request.

The The Act does not provide specific exceptions to a right to erasure.

5.2. Right to be informed

Fairly consistent

Similar to the GDPR, the Act provides that operators involved in the processing of personal data must give clarifications to the data subject regarding the processing of their personal data prior to consent collection. The Act also contains some detail on matters such as intelligibility, format, and modifications to information that must be provided to data subject. However, the Act is less detailed that the GDPR on information that must be provided to data subjects when personal data is obtained from third parties.

GDPR	Act

Informed prior to/ at collection

Article 13(1): Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
(a) the identity and the contAct details of the controller and, where applicable, of the controller's representative;
(b) the contAct details of the data protection officer, where applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, the fAct that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
(2) In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to

Section 8(1) of the Act: 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, if that is the case, to be given by that data controller a description of:
(a) the data subject's personal data;
(b) the purposes for which they are being or are to be processed by or on behalf of that data controller;
(c) the recipients or classes of recipients to whom the data are or may be disclosed by or on behalf of that data controller;
(d) any countries or territories outside the Islands to which the data controller, whether directly or indirectly, transfers, intends to transfer or wishes to transfer the data;
(e) general measures to be taken for the purpose of complying with the seventh data protection principle; and
(f) such other information as the Ombudsman may require the data controller to provide.

GDPR	Act

Informed prior to/ at collection (cont'd)

withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(d) the right to lodge a complaint with a supervisory authority;
(e) whether the provision of personal data is a statutory or contrActual requirement, or a requirement necessary to enter into a contrAct, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

What information is to be provided

See Article 13(1) and (2) above

See Section 8(1) of the Act above.
Section 5 of the Regulations: Where a request under Section 8 [of the Act] is received from a data subject, the data controller shall inform the data subject of the right to complaint to the Ombudsman under Section 43 of the [Act].
Section 9(6) of the Act: Personal data and other information supplied under Section 8 of the Act shall be supplied by reference to the data in question at the time when the request for the personal data is received, except that account may be taken of any amendment or deletion made between that time and the time when the information is supplied, the amendment or deletion being such that would have been made regardless of the receipt of the request.
Section 9(5) of the Act: Section 8(3) of the Act shall not be regarded as requiring the provision of information as to the logic of any decision-making where the information constitutes a trade secret.

When data is from third party

In addition to the information required under Article 13, Article 14(2) replaces the requirement that data subjects are provided with information on the legitimate interests pursued by the controller or by a third party, with an obligation to inform data subjects of the categories of personal data. Furthermore, paragraph (e) of Article 13(2) is replaced with a requirement to inform data subjects of the source from which the personal data originate, and if applicable, whether it came from publicly accessible sources.

The Act does not cover when data is from third parties.

GDPR	Act

Intelligibility requirements

Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Section 8(2) of the Act: A data subject is entitled to communication in an intelligible form, by the relevant data controller, of (a) the data subject's personal data; and (b) any information available to the relevant data controller as to the source of those personal data.
Section 9(2) of the Act: If any of the personal data referred to in Section 8(2)(a) of the Act are expressed in terms that are not intelligible without explanation the copy shall be accompanied by an adequate explanation.

Format

See Article 12(1) above.

Section 9(1) of the Act: The obligation imposed by Section 8(2)(a) of the Act shall be complied with by supplying the data subject with a copy of the personal data in the format requested unless: (a) the supply of such a copy is not possible or would involve disproportionate effort; or (b) the data subject agrees otherwise.

Exceptions

The requirements of Article 13 do not apply where the data subject already has the information.
The requirements of Article 14 do not apply where:
(a) the data subject already has the information;
(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

Section 8(7) of the Act: If a data controller cannot comply with the request without disclosing personal data relating to another data subject who can be identified from that personal data, the data controller is not obliged to comply with the request unless: (a) the other data subject has consented to the disclosure of the personal data to the person making the request; or (b) it is reasonable in all the circumstances to comply with the request without the consent of the other data subject.
Section 8(8) of the Act: In Section 8(7) of the Act, the reference to personal data relating to another data subject includes a reference to personal data identifying that other data subject as the source of the personal data sought in the request.
Section 8(10) of the Act: In determining for the purposes of Section 8(7)(b) of the Act whether it is reasonable in all the circumstances to comply with the request without the consent of the other data subject concerned, the data controller shall have regards to, in particular: (a) any duty of confidentiality owed to the other data subject; (b) any steps taken by the data controller to seek the consent of the other data subject; (c)

GDPR	Act

Exceptions (cont'd)

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.	whether the other data subject is capable of giving consent; and (d) any express refusal of consent by the other data subject. Section 9(3) of the Act: If a data controller has previously complied with a request under Section 8 of the Act by the data subject referred to therein, the data controller is not obliged to comply with a subsequent identical or similar request under that section by the data subject unless the interval between compliance with the previous request and the making of the current request is reasonable. Section 9(4) of the Act: In determining whether the interval referred to in Section 9(3) of the Act is reasonable, regard shall be had to the nature of the personal data, the purpose for which the personal data are processed and the frequency with which the personal data are altered.

5.3. Right to object

Fairly consistent

The Act provides data subjects with a right to object to processing; however, this right is broadly phrased, and the Act does not specify related matters in the same detail as the GDPR. Similar to the GDPR, however, the Act requires that data subjects be informed of their right to object and sets a timeframe for data controllers to respond to such requests.

GDPR	Act

Grounds for right to object/ opt out

Article 21(1): The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.	Section 10(1) of the Act: A data subject is entitled at any time, by notice in writing to a data controller, to require the 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.

Withdraw consent

Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.	Schedule 5(3) of the Act: The data subject shall have the right to withdraw consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Restrict processing

Article 18(1): The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.	See Section 10(1) of the Act above.

GDPR	Act

Object to direct marketing

GDPR	Act
Article 21(3): Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.	Section 11(2) of the Act: A data subject is entitled at any time, by notice in writing to a data controller, to require the data controller at the end of such period as is reasonable in the circumstances, to cease, or not to begin, processing for the purposes of direct marketing personal data relating to the data subject.

Inform data subject of right

GDPR	Act
See Article 12(1) in section 5.1. above. In addition, Article 21(4) provides: At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.	Section 8(12) of the Act: If personal data are being processed by or on behalf of a data controller who receives a request under this Section from the data subject, the obligation to supply the personal data under this Section includes an obligation to give the data subject a statement of the data subject's rights under the Act in such form, and to such extent, as may be prescribed by regulations.

Fees

GDPR	Act
See Article 12(5) in section 5.1. above.	The Act does not address fees in relation to the right to object.

Response timeframe

GDPR	Act
See Article 12(3) in section 5.1. above.	Section 10(2) of the Act: The data controller shall, as soon as practicable, but in any case within 21 days of receiving a notice under Section 10(1) of the Act, comply with that notice 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 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) the processing is necessary in such other circumstances as may be prescribed by regulations and the data controller shall state to the data subject the reasons for the noncompliance with the notice.

GDPR	Act

Response timeframe (cont'd)

GDPR	Act
	Section 6 of the Regulations:(1) Without limiting Sections 10(2)(a) to (c) [of the Act], a data controller shall comply with a request under Section 10(1) unless 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 to cease processing. (2) The data controller shall inform the data subject of any application made to the Ombudsman under paragraph (1).

Format of response

GDPR	Act
See Article 12(1) in section 5.1. above.	The Act does not address format of responses in relation to the right to object.

Exceptions

GDPR	Act
See Article 12(5) in section 5.1. above.	See Section 10(2) of the Act above.

5.4. Right of access

The Act, like the GDPR, establishes a right of access and details information that must be provided, as well as a timeframe for a response. It also outlines types of data that are exempt from this right. There are, however, differences in terms of informing data subjects of their rights as well as in the capacity to charge fees.

GDPR	Act

Grounds for right of access

Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.

Section 8 of the Act: (1) 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, if that is the case, to be given by that data controller a description of:
(a) the data subject's personal data;
(b) the purposes for which they are being or are to be processed by or on behalf of that data controller;
(c) the recipients or classes of recipients to whom the data are or may be disclosed by or on behalf of that data controller;
(d) any countries or territories outside the Islands to which the data controller, whether directly or indirectly, transfers, intends to transfer or wishes to transfer the data;
(e) general measures to be taken for the purpose of complying with the seventh data protection principle; and
(f) such other information as the Ombudsman may require the data controller to provide.
(2) A data subject is entitled to communication in an intelligible form, by the relevant data controller, of: (a) the data subject's personal data; and (b) any information available to the relevant data controller as to the source of those personal data.

Information to be accessed

Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
(a) the purposes of the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

See Section 8(1) and (2) of the Act above.
Section 8(3) of the Act: If the processing by automatic means of the data subject's personal data for the purpose of evaluating matters relating to the data subject, including the data subject's performance at work, creditworthiness, reliability or conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting the data subject, the data subject is entitled to be informed by the relevant data controller of the reasons for that decision.

GDPR	Act

Information to be accessed

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) the right to lodge a complaint with a supervisory authority;
(g) where the personal data are not collected from the data subject, any available information as to their source; and
(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Inform data subject of right

See Article 12(1) in section 5.1.

Section 8(12) of the Act: If personal data are being processed by or on behalf of a data controller who receives a request under this Section from the data subject, the obligation to supply the personal data under this Section includes an obligation to give the data subject a statement of the data subject's rights under the Act in such form, and to such extent, as may be prescribed by regulations.

Section 5 of the Regulations: Where a request under Section 8 [of the Act] is received from a data subject, the data controller shall inform the data subject of the right to complain to the Ombudsman under Section 43 of the Act.

Fees

See Article 12(5) in section 5.1. above.

Section 8(4) of the Act: A data controller shall not be obliged under Subsection (1), (2) or (3) to supply any personal data unless the data controller has received: (a) a request in writing; and (b) the fee that the data controller may require, such fee, being within the limits prescribed by regulations.

GDPR	Act

Fees

Section 3 of the Regulations: (1) Personal data and information pursuant to a request under Section 8 of the [Act] shall be provided free of charge, except that where the request from a data subject is determined to be manifestly unfounded or excessive because the request: (a) is repetitive; (b) is fraudulent in nature; or (c) would divert the resources of the data controller unreasonably; the data controller may charge such fee as covers the cost of providing the requested data and information or may refuse to act on the request and provide the reasons for doing so.
(2) The burden of proving that the request was 'manifestly unfounded' or 'excessive' is on the data controller.
(3) Where personal data are (a) open to access by the public pursuant to any other enactment as part of a public register or otherwise; or (b) available for purchase by the public in accordance with administrative procedures established for that purpose, access to that data shall be obtained in accordance with the provisions of that enactment or those administrative procedures.
(4) Where a data controller charges a fee pursuant to Section 3(1) of the Regulations, the fee shall be reasonable taking into account the administrative cost of providing the personal data or information requested.

Verify data subject request

Recital 64: The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

Section 8(5) of the Act: If a data controller reasonably requires further information in order to be satisfied as to the identity of the data subject making the request or to locate the information that the data subject seeks, and has informed the data subject in writing of the requirement, the data controller is not obliged to comply with the request unless supplied with that information, during which period the time specified in Section 8(6) of the Act shall automatically stand suspended.

Response timeframe

See Article 12(3) in section 5.1. above.

Section 8(6) of the Act: A data controller shall comply with a request under this Section within 30 days (or such other period as may be prescribed by regulations) of the date on which the data controller receives both the request and fee referred to

GDPR	Act

Response timeframe

in Section 8(4) of the Act, but where the data controller has requested further information under Section 8(5), of the Act the period shall not resume until the information has been supplied.
Section 4 of the Regulations: (1) A data controller may extend the time for responding to a subject access request under Section 8 of the [Act] by up to 30 days where one or more of the following conditions apply:
(a) a large amount of data is requested or is required to be searched and meeting the timelines would unreasonably interfere with the operations of the data controller;
(b) more time is required to consult with a third party or other data controller 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 has given consent to the extension.
(2) With the permission of the Ombudsman, the data controller may extend the time for responding to a subject access request under Section 8 [of the Act]: (a) for a period longer than 30 days, where one or more of the circumstances described in paragraphs (1)(a) to (c) apply; and
(b) where the Ombudsman otherwise considers that it is appropriate to do so.
(3) Where the time for responding to a request is extended under the Regulations, the data controller shall inform the data subject of the reason for the extension and when a final response will be given.

Format of response

See Article 12(1) in section 5.1. above.

Section 8(2) of the Act: A data subject is entitled to communication in an intelligible form, by the relevant data controller, of (a) the data subject's personal data; and (b) any information available to the relevant data controller as to the source of those personal data.
Section 9 of the Act: (1) The obligation imposed by Section 8(2)(a) of the Act shall be complied with by supplying the data subject with a copy of the personal data in the format requested unless: (a) the supply of such a copy is not possible or would involve disproportionate effort; or (b) the data subject agrees otherwise.
(2) If any of the personal data referred to in Section

GDPR	Act
Format of response (cont'd)	
	8(2)(a) of the Act are expressed in terms that are not intelligible without explanation the copy shall be accompanied by an adequate explanation.
Exceptions	
See Article 12(5) in section 5.1. above.	There are certain requirements and exceptions relating to providing information under Section 8 of the Act where such provision may affect multiple data subjects (see section 6.2. above). Section 9 of the Act: (3) If a data controller has previously complied with a request under Section 8 of the Act by the data subject referred to therein, the data controller is not obliged to comply with a subsequent identical or similar request under that section by the data subject unless the interval between compliance with the previous request and the making of the current request is reasonable. (4) In determining whether the interval referred to in Section9(3) of of the Act is reasonable, regard shall be had to the nature of the personal data, the purpose for which the personal data are processed and the frequency with which the personal data are altered. (5) Section 8(3) of the Act shall not be regarded as requiring the provision of information as to the logic of any decision-making where the information constitutes a trade secret. (6) Personal data and other information supplied under Section 8 of the Act shall be supplied by reference to the data in question at the time when the request for the personal data is received, except that account may be taken of any amendment or deletion made between that time and the time when the information is supplied, the amendment or deletion being such that would have been made regardless of the receipt of the request. Sections 7, 8, and 9 of the Regulations provide certain exemptions from Section 8 of the Act for personal data related to health, education, and social work respectively.

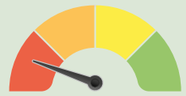
5.5. Right not to be subject to discrimination

The Act does not provide a general right not to be subject to discrimination for exercising rights. However, like the GDPR, the Act regulates against decision making by automated means.

GDPR	Act
Definition of right	
The GDPR only implies this right and does not provide an explicit definition for it.	The Act does not provide a definition of this right.
Automated processing	
Article 22(1): The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. [Article 22 goes on to detail this right, including exceptions]	Section 12 of the Act: (1) A data subject is entitled at any time, by notice in writing to a data controller, to require the 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. (2) If no notice has been given under Section 12(1) of the Act and a decision that significantly affects a data subject is based solely on processing specified in that subsection: (a) the data controller shall 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 that notification from the data controller, by notice in writing, to require the data controller to reconsider the decision or to take a new decision otherwise than on that basis. (3) The data controller shall, within 21 days of receiving a notice under Section 12(2)(b) of her Act, give the data subject a written notice specifying the steps that the data controller intends to take to comply with the notice. (4) A notice under Section 12(1) of the Act does not have effect in relation to, and nothing in Section 12(2) of the Act applies to, a decision: (a) in respect of which one condition in each of Section 12(5) and (6) is satisfied; or (b) that is made in such other circumstances as may be prescribed by regulations. (5) The first condition is that the decision: (a) is taken in the course of steps taken: (i) for the purpose 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) is authorised or required by or under any enactment.

GDPR	Act
Automated processing (cont'd)	
	(6) The second condition is that: (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 of the data subject including by allowing the data subject to make representations. (7) If the Ombudsman is satisfied on the application of a data subject that a person taking a decision in respect of the data subject has failed to comply with a notice under Section 12(1) or (2)(b) of the Act, the Ombudsman may, among other things, issue an enforcement order directing the data controller to reconsider the decision where that decision is not based solely on the processing mentioned in Section 12(1) of the Act.

5.6. Right to data portability



Unlike the GDPR, the Act does not establish a right to data portability.

GDPR	Act
Grounds for portability	
Article 20(1): The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contrAct pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means.	The Act does not provide for a right to data portability.
Inform data subject of right	
See Article 12(1) in section 5.1.	The Act does not provide for a right to data portability.
Fees	
See Article 12(5) in section 5.1. above.	The Act does not provide for a right to data portability.
Response timeframe	
See Article 12(3) in section 5.1. above.	The Act does not provide for a right to data portability.
Format	
See Article 20(1) above.	The Act does not provide for a right to data portability.
Controller to controller	
Article 20(2): In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.	The Act does not provide for a right to data portability.

GDPR	Act
Technically feasible	
See Article 20(2) above.	Not applicable
Exceptions	
See Article 12(5) in section 5.1. above.	The Act does not provide for a right to data portability.

6. Enforcement

Fairly consistent

6.1. Monetary penalties

Both the GDPR and the Act provide that data protection authorities can issue monetary penalties, however the potential sanctions under the Act are significantly smaller.

GDPR	Act
Provides for monetary penalties	
The GDPR provides for monetary penalties.	The Act provides for monetary penalties.
Issued by	
Article 58(2) Each supervisory authority shall have all of the following corrective powers: [...] (i): to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.	Section 55 of the Act: (1) The Ombudsman may serve a data controller with a monetary penalty order if the Ombudsman is satisfied on a balance of probabilities that: (a) there has been a serious contravention of the Act by the data controller; and (b) the contravention was of a kind likely to cause substantial damage or substantial distress to the data subject. (2) A monetary penalty order is an order requiring the data controller to pay a monetary penalty of an amount determined by the Ombudsman and specified in the order. [...] (5) The Ombudsman, before serving a monetary penalty order, shall serve the data controller with a notice of intent that the Ombudsman proposes to serve a monetary penalty order. (6) A notice of intent shall state that the data controller may make written representations in relation to the Ombudsman's proposal within a period of 21 days and such other information as may be prescribed. (7) The Ombudsman may not serve a monetary penalty order until the period specified in Section 55(6) of the Act has expired.
Fine maximum	
Article 83(5): infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; (b) the data subjects' rights pursuant to Articles 12 to 22;	Section 55(3) of the Act: The amount of the monetary penalty determined by the Ombudsman shall not exceed KYD 250,000 [approx. €283,870].

GDPR	Act

Fine maximum (cont'd)

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
(d) any obligations pursuant to Member State law adopted under Chapter IX;
(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).
(6) Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Percentage of turnover

Under Article 83(4), (5), and (6), fines may be issued that equate to 2% or 4% of the total worldwide annual turnover of the preceding financial year.

The Act does not provide for sanctions that equate to a percentage of turnover.

Mitigating factors

Article 83(2): When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
(b) the intentional or negligent charActer of the infringement;
(c) any Action taken by the controller or processor to mitigate the damage suffered by data subjects;
(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
(e) any relevant previous infringements by the controller or processor;
(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

Section 43 of the Act: (1) A complaint may be made to the Ombudsman by or on behalf of any person about the processing of personal data that has not been or is not being carried out in compliance with the provisions of the Act or anything required to be done pursuant to the Act.
[...] (4) The matters to which the Ombudsman may have regard in determining whether or not to conduct an investigation referred to in Section 43(1) of the Act include:
(a) the extent to which the complaint appears to the Ombudsman to raise a matter of substance;
(b) any undue delay in making the complaint;
(c) whether a complaint is frivolous or vexatious; and
(d) whether or not the person making the complaint is entitled to make a request under Section 8 of the Act in respect of the personal data in question.

GDPR	Act

Mitigating factors (cont'd)

(g) the categories of personal data affected by the infringement;
(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
(k) any other aggravating or mitigating fActor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

Imprisonment

Not applicable.

There are several provisions for imprisonment, such as:
Section 44(4) of the Act: A person who refuses or, without reasonable excuse, fails to supply information required under Section 44(1) of the Act commits an offence and is liable on conviction to a fine of KYD 100,000 [approx. €113,550] or to imprisonment for a term of five years, or both.

DPO liability

Not applicable.

Not applicable

6.2. Supervisory authority

Fairly inconsistent

Although not as detailed and far reaching as the GPDR, the Ombudsman under the Act has similar brief and some comparable powers to a supervisory authority under the GDPR.

GDPR	Act

Provides for data protection authority

Article 51(1): Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

Section 32(1) of the Act: The Ombudsman shall have all powers, direct and incidental, as are necessary or convenient to undertake the Ombudsman's functions as provided for under the Act and for purposes of this Section, the word 'functions' includes power, authority, and duty.

Investigatory powers

Article 58(1): Each supervisory authority shall have all of the following investigative powers:
(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;
(b) to carry out investigations in the form of data protection audits;
(c) to carry out a review on certifications issued pursuant to Article 42(7);
(d) to notify the controller or the processor of an alleged infringement of this Regulation;
(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

Sections 34 of the Act: The principal functions of the Ombudsman include:
(a) to hear, investigate and rule on complaints made under the Act;
(b) to monitor, investigate and report on the compliance by data controllers with their obligations under the Act.
Section 43(3) of the Act: On receiving a complaint referred to in Section 43(1) of the Act, or on the Ombudsman's own motion, the Ombudsman may conduct an investigation.
Section 44(1) of the Act: The Ombudsman may require any person to provide such information as the Ombudsman may reasonably consider appropriate for the purpose of carrying out the Ombudsman's functions under the Act including any information with respect to which an exemption is claimed.
Section 51(3) of the Act: A warrant granted under Section 53(2) of the Act may authorise the Ombudsman or any of the Ombudsman's staff at any time: (a) to enter the premises and search them; (b) to inspect, examine, operate and test any equipment found there which is used or intended to be used for the processing of personal data; and (c) to inspect, examine and seize any documents, equipment or other thing found there which may be evidence of the contravention of Section 51(2) of the Act.

GDPR	Act

Corrective powers

Article 58(2): Each supervisory authority shall have all of the following corrective powers:
(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
(e) to order the controller to communicate a personal data breach to the data subject;
(f) to impose a temporary or definitive limitation including a ban on processing;
(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such Actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;
(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

Sections 34 of the Act: The principal functions of the Ombudsman include:
[...] (c) to intervene and deliver opinions and orders related to processing operations;
(d) to order the rectification, blocking, erasure or destruction of data;
(e) to impose a temporary or permanent ban on processing;
(f) to make recommendations for reform both of a general nature and directed at specific data controllers;
(g) to engage in proceedings where the provisions of the Act have been violated, or refer these violations to the appropriate authorities.
Section 45(1): If the Ombudsman is satisfied that there are reasonable grounds for believing that a data controller has contravened, is contravening or is likely to contravene any provision of the Act, the Ombudsman may, with a view to effecting the data controller's compliance with the provision, by way of an order served on the data controller, require that data controller to:
(a) take specified steps within a specified time, or to refrain from taking specified steps after a specified time;
(b) refrain from processing any personal data, or any personal data of a specified description;
(c) refrain from processing data for a specified purpose or in a specified manner, after a specified time; or
(d) do anything which appears to the Ombudsman to be incidental or conducive to the carrying out of the Ombudsman's functions under the Act.

GDPR	Act

Authorisation/ advisory powers

Article 58(3): Each supervisory authority shall have all of the following authorisation and advisory powers: (a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36; (b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data; (c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation; (d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5); (e) to accredit certification bodies pursuant to Article 43; (f) to issue certifications and approve criteria of certification in accordance with Article 42(5); (g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2); (h) to authorise contrActual clauses referred to in point (a) of Article 46(3); (i) to authorise administrative arrangements referred to in point (b) of Article 46(3); (j) to approve binding corporate rules pursuant to Article 47.	Sections 34 of the Act: The principal functions of the Ombudsman include: [...] (h) to co-operate with other data protection supervisory authorities; (i) to publicise and promote the requirements of the Act and the rights of data subjects under it; and (j) to do anything which appears to the Ombudsman to be incidental or conducive to the carrying out of the Ombudsman's functions under the Act. Section 42(1) of the Act: The Cabinet may, after consulting with the Ombudsman, make regulations for the preparation and dissemination of codes of practice which may be specific to a particular industry or processing operation. [...] (3) The Ombudsman shall also: (a) if the Ombudsman considers it appropriate to do so, encourage trade associations to prepare, and to disseminate to their members, codes of practice for guidance as to good practice; and (b) if a trade association submits a code of practice for the Ombudsman's consideration, consider the code and, after such consultation with data subjects or persons representing data subjects as appears to the Ombudsman to be appropriate, notify the trade association whether, in the Ombudsman's opinion, the code promotes good practice. (4) The Ombudsman may, with the consent of the relevant data controller, assess any processing of personal data for the adherence to good practice and shall inform the data controller of the results of the assessment.

Tasks of authority

Article 57(1): Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: (a) monitor and enforce the application of this Regulation; (b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention; (c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;	See Section 34 of the Act above.

GDPR	Act

Tasks of authority

(d) promote the awareness of controllers and processors of their obligations under this Regulation; (e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end; (f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary; (g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation; (h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority; (i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices; (j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2); (k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4); (l) give advice on the processing operations referred to in Article 36(2); (m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5); (n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5); (o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7); (p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;	Please see Article 18(3) above.

GDPR	Act

Tasks of authority (cont'd)

(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
(r) authorise contrActual clauses and provisions referred to in Article 46(3);
(s) approve binding corporate rules pursuant to Article 47;
(t) contribute to the Activities of the Board;
(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and
(v) fulfil any other tasks related to the protection of personal data.

Annual report

Article 59: Each supervisory authority shall draw up an annual report on its Activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

Section 36 of the Act: The Ombudsman shall, as soon as reasonably practicable after the end of each year, lay before the Cayman Islands Parliament: (a) a report of the operation of the Act during the year and may from time to time submit such other reports as the Ombudsman thinks appropriate.

6.3. Civil remedies for individuals

Fairly inconsistent

The Act provides data subjects with the right to pursue civil remedies but, unlike the GDPR, the Act does not detail this right.

GDPR	Act

Provides for claims/ cause of Action

Article 79: Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

Section 13 of the Act: A person who suffers damage by reason of a contravention by a data controller of any requirement of the Act has a cause of action for compensation from the data controller for that damage.

Material and non-material damage

Article 82(1): Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

The Act does not define whether damage can be material and non-material.

Mandate for representation

Article 80(1): The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is Active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

The Act does not provide a mandate for representation.

Specifies amount for damages

Not applicable.

The Act does not specify amount for damages.

GDPR	Act
Processor liability	
Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.	The Act does not define data processor liabilities.
Exceptions	
Article 82(3): A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.	The Act does not provide specific exemptions from liabilities.