Comparing privacy laws:
GDPR v. Kenya Data Protection Act

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

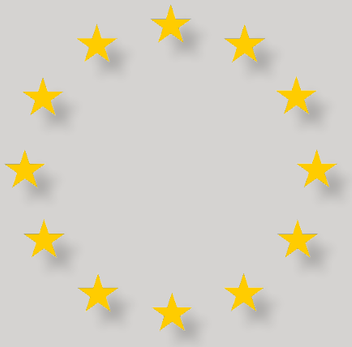
OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

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 regulations 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, 2019 ('the Act'), which came into force on 25 November 2019, is the primary piece of data protection legislation in Kenya. The Act provides for the establishment of the Data Protection Office ('ODPC') to enforce its provisions, however this office has yet to be formed.

The Act has many similarities with the GDPR and often uses the same general concepts as well as the same language on occasion. While these foundations are largely mirrored between the two pieces of legislation, there are several key, nuanced differences. For instance, the Act provides less detailed information on the exercise of data subject rights, broader data transfer obligations, and registration rather than record keeping obligations. Furthermore, the Act specifies at various points that the ODPC will issue further guidance.

Further to the above, the ODPC issued, in early April 2020, three draft data protection regulations (combined in one document) (collectively 'the Draft Regulations'), which if passed, will form part of the Act. The Draft Regulations are:

- the Data Protection (General) Regulations, 2021 ('the Draft General Regulations');
- the Data Protection (Compliance and Enforcement) Regulations 2021 ('the Draft Enforcement Regulations'); and
- the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.

The Draft Regulations provide more detail on the general enforcement of the Act, as well as particular requirements and obligations on data controllers and data processors.

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.

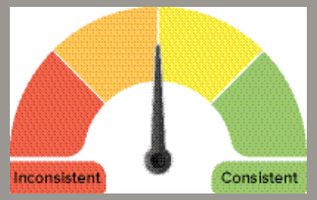
Key for giving the consistency rate

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

1.1. Personal scope

The Act establishes similar central concepts of data controllers, data processors, and data subjects. However, it is less explicit than the GDPR in relation to the nationality and place of residence of data subjects, and does not directly address deceased person's data.

GDPR	The 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: 'data controller' means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data.
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: 'data processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf 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: 'data subject' means an identified or identifiable natural person who is the subject of personal data. Section 2: 'identifiable natural person' means a person who can be identified directly or indirectly, 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 or social identity.
Public bodies	
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body.	The definitions of a 'data controller' and 'data processor' in Section 2 includes public authorities.

GDPR	The 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.	Section 4: This Act applies to the processing of personal data - (a) entered in a record, by or for a data controller or processor, by making use of automated or nonautomated means: Provided that when the recorded personal data is processed by non-automated means, it forms a whole or part of a filing system; (b) by a data controller or data processor who - (i) is established or ordinarily resident in Kenya and processes personal data while in Kenya; or (ii) not established or ordinarily resident in Kenya, but processing personal data of data subjects located in Kenya.
Place of residence	
See Recital 14, above.	See Section 4 of the Act above.
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.	The Act does not explicitly refer to deceased individual's data.

1.2. Territorial scope

Both the GDPR and the Act regulate organisations established within the respective jurisdictions. The Act, though, provides for a broader extraterritorial scope and applies to any controller or processor processing data of Kenyan citizens, regardless of whether the controller or processor is established in Kenya or their specific processing activities.

GDPR	The 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 4: This Act applies to the processing of personal data – (a) entered in a record, by or for a data controller or processor, by making use of automated or nonautomated means: Provided that when the recorded personal data is processed by non-automated means, it forms a whole or part of a filing system; (b) by a data controller or data processor who - (i) is established or ordinarily resident in Kenya and processes personal data while in Kenya; or (ii) not established or ordinarily resident in Kenya, but processing personal data of data subjects located in Kenya.
Extraterritorial	
See Article 3, above.	See Section 4(b)(ii) 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 explicitly refer to goods and services from abroad, however see Section 4(b)(ii) above.
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 explicitly refer to monitoring from abroad, however see Section 4(b)(ii), above.

1.3. Material scope

Fairly consistent

There are several general similarities between the GDPR and the Act, including that they both explicitly consider anonymised and pseudonymised data, apply to automated processing, and have comparable concepts of personal data and sensitive data. However, there are key differences in regard to how the anonymisation is referred to and in what types of data are considered personal data, with the Act providing including matters such as family members' names.

GDPR	The 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: 'personal data' means any information relating to an identified or identifiable natural person.

Section 2: 'identifiable natural person' means a person who can be identified directly or indirectly, 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 or social identity.

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: 'processing' means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as

(a) collection, recording, organisation, structuring;

(b) storage, adaptation or alteration;

(c) retrieval, consultation or use;

(d) disclosure by transmission, dissemination, or otherwise making available; or

(e) alignment or combination, restriction, erasure or destruction.

GDPR	The Act

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 2: 'sensitive personal data' means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject. [Sections 44-48 of the Act regulate the processing of sensitive data.]

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.

Section 2: 'anonymisation' means the removal of personal identifiers from personal data so that the data subject is no longer identifiable.

Section 37(2): A data controller or data processor that uses personal data for commercial purposes shall, where possible, anonymise the data in such a manner as to ensure that the data subject is no longer identifiable.

Section 39(2): A data controller or data processor shall delete, erase, anonymise or pseudonymise personal data not necessary to be retained under sub-section (1) in a manner as may be specified at the expiry of the retention period.

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.

Section 2: '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, and such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

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.

Section 4: This Act applies to the processing of personal data - (a) entered in a record, by or for a data controller or processor, by making use of automated or nonautomated means:

Provided that when the recorded personal data is processed by non-automated means, it forms a whole or part of a filing system;

GDPR	The Act
Automated processing (cont'd)	
	(b) by a data controller or data processor who - (i) is established or ordinarily resident in Kenya and processes personal data while in Kenya; or (ii) not established or ordinarily resident in Kenya, but processing personal data of data subjects located in Kenya.
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.	Section 51: (2) The processing of personal data is exempt from the provisions of this Act if – (a) it relates to processing of personal data by an individual in the course of a purely personal or household activity; (b) if it is necessary for national security or public interest; or (c) disclosure is required by or under any written law or by an order of the court. [Sections 52 and 53 provide further exceptions for journalism, literature, and art, as well as research and statistics]

2. Key definitions

2.1. Personal data

Definitions within the GDPR and the Act are relatively similar in relation to personal data and associated terms, and in some cases the Act directly mirrors the GDPR. However, there are slight differences, for example in relation to the specific categories of sensitive data.

GDPR	The 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: 'personal data' means any information relating to an identified or identifiable natural person. Section 2: 'identifiable natural person' means a person who can be identified directly or indirectly, 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 or social identity.
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 2: 'sensitive personal data' means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject.
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.	See the definition of 'identifiable natural person' above, which includes reference to 'online identifiers'.

GDPR	The Act
Filing system	
The GDPR does not provide for a definition of 'data collector'.	Section 2: 'filing system' means any structured set of personal data which is readily accessible by reference to a data subject or according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
Profiling	
Article 4(9): 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. 2However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.	Section 2: 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth; personal preferences, interests, behaviour, location or movements.
Third Party	
Article 4(9): 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. 2However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.	Section 2: 'third party' means natural or legal person, public authority, agency or other body, other than the data subject, data controller, data processor or persons who, under the direct authority of the data controller or data processor, are authorised to process personal data.

2.2. Pseudonymisation

The definitions of anonymisation and pseudonymisation are essentially the same, although the Act refers to the act of anonymisation while the GDPR refers to anonymous information.

GDPR	The 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.	Section 2: 'anonymisation' means the removal of personal identifiers from personal data so that the data subject is no longer identifiable.
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.	Section 2: '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, and such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

2.3. Controllers and processors

The definitions for data controllers and processors as well as associated activities are very similar between the GDPR and the Act. The most notable difference is that the Act provides less detail in regard to the content of contracts between data controllers and processors, although it still requires a written contract to be in place.

GDPR	The 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: 'data controller' means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data.

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: 'data processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf 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.]

Section 42: (2) Where a data controller is using the services of a data processor - (a) the data controller shall opt for a data processor who provides sufficient guarantees in respect of organisational measures for the purpose of complying with Section 41(1); and

(b) the data controller and the data processor shall enter into a written contract which shall provide that the data processor shall act only on instructions received from the data controller and shall be bound by obligations of the data controller.

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).

Section 31(4): For the purposes of this Section, a 'data protection impact assessment' means an assessment of the impact of the envisaged processing operations on the protection of personal data. (see section 4.3. below for further information).

GDPR	The Act

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).

DPO is not specifically defined, however Section 24 sets out requirements related to DPOs (see section 4.4. for further information).

2.4. Children

While both the GDPR and the Act consider special requirements for the processing of children's data, they do so in different ways. The Act more generally discusses the processing of children's data and explicitly considers mechanisms for verification of age and consent.

GDPR	The 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.

The Act does not specifically define 'child'. However, Section 33 provides detailed requirement for processing children's data. [Note: Article 260 of the Kenyan Constitution stipulates the age threshold for adulthood to be 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.

Section 33: (1) Every data controller or data processor shall not process personal data relating to a child unless - (a) consent is given by the child's parent or guardian; and
(b) the processing is in such a manner that protects and advances the rights and best interests of the child.
(2) A data controller or data processor shall incorporate appropriate mechanisms for age verification and consent in order to process personal data of a child.
(3) Mechanisms contemplated under sub-section (2) shall be determined on the basis of - (a) available technology;
(b) volume of personal data processed;
(c) proportion of such personal data likely to be that of a child;
(d) possibility of harm to a child arising out of processing of personal data; and
(e) such other factors as may be specified by the Data Commissioner.
(4) A data controller or data processor that exclusively provides counselling or child protection services to a child may not be required to obtain parental consent as set out under sub-section (1).

GDPR	The Act

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 explicitly refer to privacy notices for processing children's data.

2.5. Research

Fairly consistent

While both the GDPR and the Act provide exceptions for processing conducted for research purposes, including requirements for research as further processing and appropriate safeguards, there are differences in relation to data subject rights. The Act, though, stipulates that the Data Commissioner should issue a relevant code of practice.

GDPR	The 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.

Although the Act provides requirements and exceptions for processing for the purposes of research, history, and statistics, it does not explicitly define these 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 53(1): The further processing of personal data shall be compatible with the purpose of collection if the data is used for historical, statistical or research purposes and the data controller or data processor shall ensure that the further processing is carried out solely for such purposes and will not be published in an identifiable form.

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 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.

Section 53: (2) The data controller or data processor shall take measures to establish appropriate safeguards against the records being used for any other purposes.

(3) Personal data which is processed only for research purposes is exempt from the provisions of this Act if - (a) data is processed in compliance with the relevant conditions; and (b) results of the research or resulting statistics are not made available in a form which identifies the data subject or any of them.

GDPR	The Act

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.

The Act does not set out particular requirements for data subject rights in the context of research. Section 53(4), though, provides that: The Data Commissioner shall prepare a code of practice containing practical guidance in relation to the processing of personal data for purposes of Research, History and Statistics.

3. Legal basis

Fairly consistent

The GDPR and the Act set out very similar legal bases for processing both personal data and sensitive data, comparable conditions of consent, and exceptions for processing for journalism or artistic purposes. There are, however, slight differences in regard to the withdrawal of consent and consent in relation to the performance of a contract.

GDPR	The Act

Legal grounds

GDPR	The Act
Article 6(1): Processing shall be lawful only if and to the extent that at least one of the following applies:	Section 30: (1) A data controller or data processor shall not process personal data, unless - (a) the data subject consents to the processing for one or more specified purposes; or
(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;	(b) the processing is necessary -
(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;	(i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;	(ii) for compliance with any 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;	(iii) in order to protect the vital interests of the data subject or 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	(iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(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.	(v) the performance of any task carried out by a public authority;
	(vi) for the exercise, by any person in the public interest, of any other functions of a public nature;
	(vii) for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or
	(viii) for the purpose of historical, statistical, journalistic, literature and art or scientific research.

GDPR	The Act

Sensitive data (legal basis)

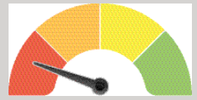
GDPR	The Act
There are specific requirements for processing special categories of data, see Article 9 of the GDPR for further information.	There are specific requirements for processing sensitive data, see Section 45 of the Act for further information.

Conditions for consent

GDPR	The Act
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.	Section 32: (1) A data controller or data processor shall bear the burden of proof for establishing a data subject's consent to the processing of their personal data for a specified purpose.
	(2) Unless otherwise provided under this Act, a data subject shall have the right to withdraw consent at any time.
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.	(3) The withdrawal of consent under sub-section (2) shall not affect the lawfulness of processing based on prior consent before its withdrawal.
	(4) In determining whether consent was freely given, account shall be taken of whether, among others, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.
	Section 4 of the Draft General Regulations: (3) In obtaining consent from a data subject, a data controller or a data processor shall ensure that the —
	(a) data subject has capacity to understand and communicate their consent;
	(b) data subject is informed of the nature of processing in simple and clear language that is understandable;
	(c) data subject voluntarily gives consent; and
	(d) consent is specific.
	(4) A data subject may prior to the processing of their personal data give consent either orally or in writing, and may include a handwritten signature, an oral statement, or use of an electronic or other medium to signify agreement.

GDPR	The Act
Conditions for consent (cont'd)	
	(5) A data controller or data processor shall not presume that a data subject has given consent on the basis that the data subject did not object to a proposal to handle their personal data in a particular manner. (6) Consent shall not be implied, where the intention of the data subject is ambiguous or there is reasonable doubt as to the intention of the data subject. (7) Subject to Section 32(2) and (3) of the Act, a data subject shall be informed of the implications of providing, withholding or withdrawing consent.
Legal grounds	
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 52: (1) The principles of processing personal data shall not apply where - (a) processing is undertaken by a person for the publication of a literary or artistic material; (b) data controller reasonably believes that publication would be in the public interest; and (c) data controller reasonably believes that, in all the circumstances, compliance with the provision is incompatible with the special purposes. (2) Subsection (1) (b) shall only apply where it can be demonstrated that the processing is in compliance with any self-regulatory or issued code of ethics in practice and relevant to the publication in question. (3) The Data Commissioner shall prepare a code of practice containing practical guidance in relation to the processing of personal data for purposes of Journalism, Literature and Art.

4. Controller and processor obligations



Inconsistent

4.1. Data transfers

The Act takes an alternative approach to data transfers than the GDPR, by generally requiring that data controllers or processors demonstrate to the Data Commissioner that there are appropriate safeguards unless consent has been obtained from the data subject. The Act does not explicitly define what would constitute 'appropriate safeguards'. The Act also leaves room for the Cabinet Secretary to establish data localisation / residency requirements.

GDPR	The 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.	Section 48: A data controller or data processor may transfer personal data to another country only where – (a) the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data; (b) the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including jurisdictions with commensurate data protection laws. Section 49: (1) The processing of sensitive personal data out of Kenya shall only be effected upon obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards. (2) The Data Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the security safeguards or the existence of compelling legitimate interests. (3) The Data Commissioner may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as may be determined. Section 40 of the Draft General Regulations: A data controller or data processor who is a transferring entity shall before transferring personal data out of Kenya ascertain that the transfer is based on:

GDPR	The Act

Adequate protection (cont'd)

(a) appropriate data protection safeguards;

(b) an adequacy decision made by the Data Commissioner;

(c) transfer as a necessity; or

(d) consent of the data subject.

Section 41 of the Draft General Regulations : (1) A transfer of personal data to another country or a relevant international organisation is based on the existence of appropriate safeguards where -

(a) a legal instrument containing appropriate safeguards for the protection of personal data binding the intended recipient that is essentially equivalent to the protection under the Act and these Regulations; or

(b) the data controller, having assessed all the circumstances surrounding transfers of that type of personal data to another country or relevant international organisation, concludes that appropriate safeguards exist to protect the data.

Section 42 of the Draft General Regulations: For the purpose of confirming the existence of appropriate data protection safeguards anticipated under section 49(1) of the Act, any country or a territory is taken to have such safeguards if that country or territory has —

(a) ratified the African Union Convention on Cyber Security and Personal Data Protection;

(b) reciprocal data protection agreement with Kenya; or

(c) a contractual binding corporate rules among a concerned group of undertakings or enterprises.

[Note: Sections 43 to 47 of the Draft General Regulatitons provide further detail on each of the transfer methods noted in Section 40 of the same.

GDPR	The Act

Other mechanisms for data transfers (cont'd)

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);
(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 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.

Section 48: A data controller or data processor may transfer personal data to another country only where -

[...] (c) the transfer is necessary - (i) for the performance of a contract between the data subject and the data controller or data processor or implementation of precontractual measures taken at the data subject's request;

(ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;

(iii) for any matter of public interest;

(iv) for the establishment, exercise or defence of a legal claim;

(v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(vi) for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

Section 48 of the Draft General Regulations: A transferring entity may enter into a written agreement with the recipient of personal data, which contract shall contain provisions relating to —

(a) the unlimited access by the transferring entity to ascertain the existence of a robust information system of the recipient for storing the personal data; and

(b) the countries and territories to which the personal data may be transferred under the contract.

GDPR	The Act
Data localisation	
Not applicable.	Section 50: The Cabinet Secretary may prescribe, based on grounds of strategic interests of the state or protection of revenue, certain nature of processing that shall only be effected through a server or a data centre located in Kenya. Section 25 of the General Regulations: (1) Pursuant to Section 50 of the Act, a data controller or data processor who processes personal data for the purpose of actualising a public good set out under Section 50(2) shall be required to ensure that — (a) such processing is effected through a server and data centre located in Kenya; and (b) at least one serving copy of the concerned personal data is stored in a data centre located in Kenya. (2) The purposes contemplated under paragraph (1) that require processing in Kenya include — (a) administering a national civil registration system including registrations of births and deaths, persons, adoption and marriages; (b) operating a population register and identity management system including any issuance of any public document of identity; (c) managing personal data to facilitate access of primary and secondary education in the country; (d) the conduct of elections in the country; (e) managing any electronic payments systems licensed under the National Payment Systems Act; (f) any revenue administration system for public finances; (g) processing health data for any other purpose other than providing health care directly to a data subject; or (h) managing any system designated as a protected computer system in terms of Section 20 of the Computer Misuse and Cybercrime Act, 2018. (3) Despite paragraph (2), the Cabinet Secretary may require a data controller who processes personal data outside Kenya to comply with paragraph (1), if the data controller — (a) has been notified that personal data outside Kenya has been breached or its services have been used to violate the Act and has not taken measures to stop or handle the violation; and (b) resists, obstructs or fails to comply with requests of the Data Commissioner or any other relevant authority in — (i) cooperating to investigate and handle such violations; or (ii) neutralise and disable the effect of cyber security protection measures.

4.2. Data processing records

Unlike the GDPR, the Act establishes general processing registration / notification requirements and does not explicitly require records of processing.

GDPR	The 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 explicitly provide for processing record keeping obligations.

GDPR	The 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 explicitly provide for equivalent record keeping obligations.

Records format

Article 30(3): The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.	The Act does not explicitly provide for equivalent record keeping obligations.

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 57: (1) The Data Commissioner may, for the purpose of the investigation of a complaint, order any person to – [...] (b) produce such book, document, record or article as may be required with respect to any matter relevant to the investigation, which the person is not prevented by any other enactment from disclosing; [...] (2) Where material to which an investigation relates consists of information stored in any mechanical or electronic device, the Data Commissioner may require the person named to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

Required to make available (cont'd)

	(3) A person who, without reasonable excuse, fails or refuses to comply with a notice, or who furnishes to the Data Commissioner any information which the person knows to be false or misleading, commits an offence.

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 explicitly provide for equivalent record keeping obligations.

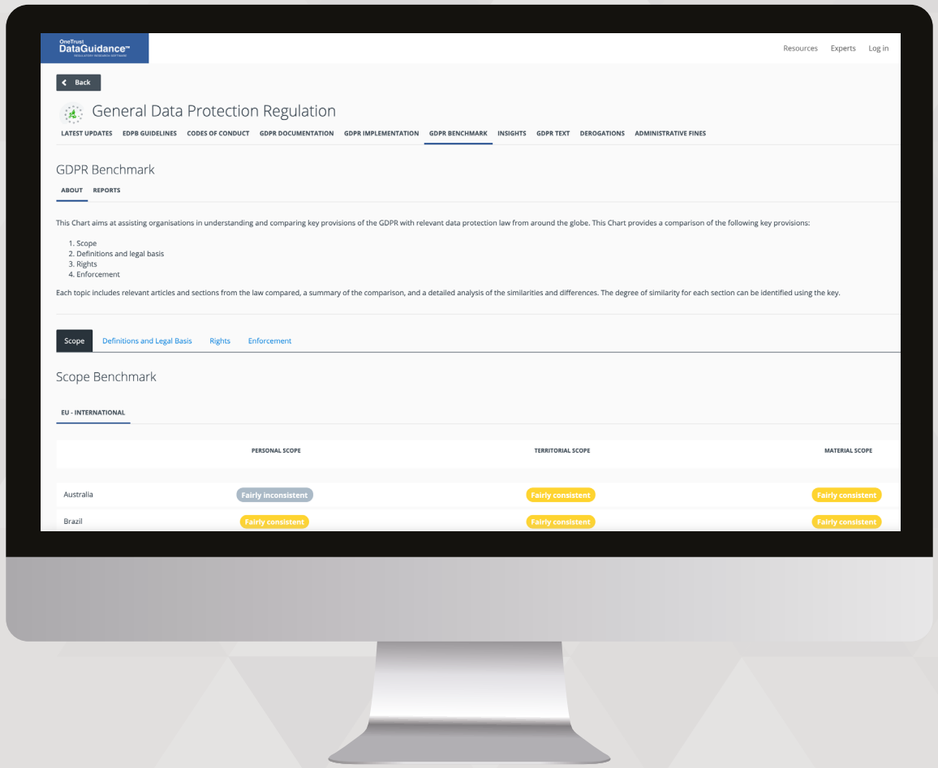
General Data Processing Notification ('DPN')

Not applicable.	Section 18: (1) Subject to sub-section (2), no person shall act as a data controller or data processor unless registered with the Data Commissioner. (2) The Data Commissioner shall prescribe thresholds required for mandatory registration of data controllers and data processors, and in making such determination, the Data Commissioner shall consider - (a) the nature of industry; (b) the volumes of data processed; (c) whether sensitive personal data is being processed; and (d) any other criteria the Data Commissioner may specify. [Note: the Act goes on to detail these registration requirements further in Sections 19-22. See Kenya - Data Processing Notification for further information].

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

4.3. Data protection impact assessment

Although the Act is less detailed, it contains broadly similar provisions to the GDPR in relation to DPIAs. This includes potential prior consultation and obligations to conduct DPIAs when processing is likely to result in high risks to data subjects.

GDPR	The 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.

Section 31(1): Where a processing operation is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context and purposes, a data controller or data processor shall, prior to the processing, carry out a data protection impact assessment.

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;

Section 31(2): A data protection impact assessment shall include the following - (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller or data processor;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

GDPR	The Act

DPIA content requirements (cont'd)

(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 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.

(c) an assessment of the risks to the rights and freedoms of data subjects;

(d) the measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act, 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].

Section 31(3): The data controller or data processor shall consult the Data Commissioner prior to the processing if a data protection impact assessment prepared under this section indicates that the processing of the data would result in a high risk to the rights and freedoms of a data subject.

[...] (5) The data impact assessment reports shall be submitted sixty days prior to the processing of data.

(6) The Data Commissioner shall set out guidelines for carrying out an impact assessment under this section.

Section 52 of the Draft General Regulations: (1) In conducting a data protection impact assessment, a data controller or a data processor may consult the Office for advice on whether risks identified and mitigation measures suggested are viable in the outlined circumstances.

4.4. Data protection officer appointment

The concepts of DPOs, their tasks, and the associated provisions regulating the appointment of DPOs are very similar between the GDPR and the Act. The primary difference is that the Act uses different language and terms such as 'may' rather than 'shall'.

GDPR	The Act

DPO tasks

GDPR	The Act
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.	Section 24(7): A data protection officer shall - (a) advise the data controller or data processor and their employees on data processing requirements provided under this Act or any other written law; (b) ensure on behalf of the data controller or data processor that this Act is complied with; (c) facilitate capacity building of staff involved in data processing operations; (d) provide advice on data protection impact assessment; and (e) co-operate with the Data Commissioner and any other authority on matters relating to data protection. Section 24(2): A data protection officer may be a staff member of the data controller or data processor and may fulfil other tasks and duties provided that any such tasks and duties do not result in a conflict of interest.

When is a DPO required

GDPR	The Act
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;	Section 24(1): A data controller or data processor may designate or appoint a data protection officer on such terms and conditions as the data controller or data processor may determine, where - (a) the processing is carried out by a public body or private body, except for courts acting in their judicial capacity;

When is a DPO required (cont'd)

GDPR	The Act
(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 (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.	(b) the core activities of the data controller or data processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects; or (c) the core activities of the data controller or the data processor consist of processing of sensitive categories of personal data.

Group appointments

GDPR	The Act
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.	Section 24: (3) A group of entities may appoint a single data protection officer provided that such officer is accessible by each entity. (4) Where a data controller or a data processor is a public body, a single data protection officer may be designated for several such public bodies, taking into account their organisational structures.

Notification of DPO

GDPR	The Act
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.	Section 24(6): A data controller or data processor shall publish the contact details of the data protection officer on the website and communicate them to the Data Commissioner who shall ensure that the same information is available on the official website.

Qualifications

GDPR	The Act
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.	Section 24(5): A person may be designated or appointed as a data protection officer, if that person has relevant academic or professional qualifications which may include knowledge and technical skills in matters relating to data protection.

4.5. Data security and data breaches

Fairly consistent

The Act and the GDPR have broadly similar security requirements with both establishing principles of Privacy by Default and by Design. They also have comparable data breach notification obligations, such as notifying authorities within 72 hours. However, some of the details within the provisions vary.

In addition, the Draft General Regulations further clarify what would constitute a notifiable data breach under the Act and outline the information that should be included in a notification.

GDPR	The 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.

Section 41: (1) Every data controller or data processor shall implement appropriate technical and organisational measures which are designed - (a) to implement the data protection principles in an effective manner; and (b) to integrate necessary safeguards for that purpose into the processing.
(2) The duty under subsection (1) applies both at the time of the determination of the means of processing the data and at the time of the processing.
(3) A data controller or data processor shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose is processed, taking into consideration
(a) the amount of personal data collected;
(b) the extent of its processing;
(c) the period of its storage;
(d) its accessibility; and
(e) the cost of processing data and the technologies and tools used.
(4) To give effect to this section, the data controller or data processor shall consider measures such as - (a) to identify reasonably foreseeable internal and external risks to personal data under the person's possession or control;
(b) to establish and maintain appropriate safeguards against the identified risks;
(c) to the pseudonymisation and encryption of personal data;
(d) to the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(e) to verify that the safeguards are effectively implemented; and
(f) to ensure that the safeguards are continually updated in response to new risks or deficiencies.
[Section 42 sets out further criteria for assessing organisational measures, and particularly in relation to data processors]

GDPR	The Act

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 43(1): Where personal data has been accessed or acquired by an unauthorised person, and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorised access, a data controller shall - (a) notify the Data Commissioner without delay, within seventy-two hours of becoming aware of such breach.
[...] (5) The notification and communication referred to under subsection (1) shall provide sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach, including - (a) description of the nature of the data breach;
(b) description of the measures that the data controller or data processor intends to take or has taken to address the data breach;
(c) recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise;
(d) where applicable, the identity of the unauthorised person who may have accessed or acquired the personal data; and
(e) the name and contact details of the data protection officer where applicable or other contact point from whom more information could be obtained.
[...] (8) The data controller shall record the following information in relation to a personal data breach - (a) the facts relating to the breach; (b) its effects; and (c) the remedial action taken.
Section 37 of the Draft General Regulations: (1) For the purpose of section 43 of the Act, a data breach is taken to result in real risk of harm to a data subject if that data breach relates to —
(a) the data subject's full name or identification number and any of the personal data or classes of personal data relating to the data subject set out in the Second Schedule; or
(b) the following personal data relating to a data subject's account with a data controller or data processor —
(i) the data subject's account identifier, such as an account name or number; and
Section 38 of the Draft General Regulations: (1) A notification by data controller or data processor to the Data Commissioner of a notifiable data breach under Section 43 of the Act shall include - (a) the date on which and the circumstances in which the data controller or data processor first became aware that the data breach had occurred;
(ii) any password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to or use of the individual's account.

GDPR	The Act

Data breach notification to authority (cont'd)

(2) A breach of any personal data envisaged under paragraph (1) amounts to notifiable data breach under Section 43 of the Act.
Section 38 of the Draft General Regulations: (1) A notification by data controller or data processor to the Data Commissioner of a notifiable data breach under Section 43 of the Act shall include - (a) the date on which and the circumstances in which the data controller or data processor first became aware that the data breach had occurred;
(b) a chronological account of the steps taken by the data controller or data processor after the data controller or data processor became aware that the data breach had occurred, including the data controller or data processor's assessment that the data breach is a notifiable data breach;
(c) details on how the notifiable data breach occurred, where applicable;
(d) the number of data subjects or other persons affected by the notifiable data breach;
(e) the personal data or classes of personal data affected by the notifiable data breach;
(f) the potential harm to the affected data subjects as a result of the notifiable data breach;
(g) information on any action by the data controller or data processor, whether taken before or to be taken after the data controller or data processor notifies the Data Commissioner of the occurrence of the notifiable data breach to —
(i) eliminate or mitigate any potential harm to any affected data subject or other person as a result of the notifiable data breach; and
(ii) address or remedy any failure or shortcoming that the data controller or data processor believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach;
(h) all or any affected individuals or the public that the notifiable data breach has occurred and how an affected data subject may eliminate or mitigate any potential harm as a result of the notifiable data breach;
(i) contact information of an authorized representative of the data controller or data processor.
(2) Where, despite Section 43(1)(b) of the Act, data controller or data processor does not intend to communicate to a data subject affected by a notifiable data breach, the notification to the Data Commissioner under paragraph (1) shall additionally specify the grounds for not notifying the affected data subject.

GDPR	The Act

Timeframe for breach notification

See Article 33(1) above.

Section 43(1): Where personal data has been accessed or acquired by an unauthorised person, and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorised access, a data controller shall - (a) notify the Data Commissioner without delay, within seventy-two hours of becoming aware of such breach.
[...] (2) Where the notification to the Data Commissioner is not made within seventy-two hours, the notification shall be accompanied by reasons for the delay.

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.

Section 43: (1) Where personal data has been accessed or acquired by an unauthorised person, and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorised access, a data controller shall -
[...] (b) subject to subsection (3), communicate to the data subject in writing within a reasonably practical period, unless the identity of the data subject cannot be established.

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.

Section 43(3): Where a data processor becomes aware of a personal data breach, the data processor shall notify the data controller without delay and where reasonably practicable, within forty-eight hours of becoming aware of such breach.

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 43: (6) The communication of a breach to the data subject shall not be required where the data controller or data processor has implemented appropriate security safeguards which may include encryption of affected personal data.
(7) Where and to the extent that it is not possible to provide all the information mentioned in subsection (5) at the same time, the information may be provided in phases without undue delay.

4.6. Accountability

Fairly consistent

Although the Act does not contain an explicit accountability principle like the GDPR, it does establish relevant provisions and provides a clear distinction of controller and processor liabilities.

GDPR	The 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 specifically define a principle of accountability, although many of its provisions may be considered to relate to accountability expectations.
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.	Section 65: (1) A person who suffers damage by reason of a contravention of a requirement of this Act is entitled to compensation for that damage from the data controller or the data processor. (2) Subject to subsection (1) - (a) a data controller involved in processing of personal data is liable for any damage caused by the processing; and (b) a data processor involved in processing of personal data is liable for damage caused by the processing only if the processor - (i) has not complied with an obligation under the Act specifically directed at data processors; or (ii) has acted outside, or contrary to, the data controller's lawful instructions.

5. Rights

Fairly consistent

5.1. Right to erasure

Like the GDPR, the Act provides data subjects with the capacity to request the erasure of data that the data controller or processor is no longer authorised to retain, irrelevant, excessive or obtained unlawfully.

Notably, the Draft General Regulation provides some further detail with regards to the right to erasure.

GDPR	The 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 40(1)(b): A data subject may request a data controller or data processor to erase or destroy without undue delay personal data that the data controller or data processor is no longer authorised to retain, irrelevant, excessive or obtained unlawfully. Section 12(1) of the Draft General Regulations: Pursuant to section 40(1)(b) of the Act, a data subject has the right to have their personal data erased if— (a) the personal data is no longer necessary for the purpose which it was originally collected; (b) the data subject withdraws their consent that was the lawful basis for retaining the personal data; (c) the data subject objects to the processing of their data and there is no overriding legitimate interest to continue the processing; (d) the processing of personal data is for direct marketing purposes and the individual objects to that processing; (e) the processing of personal data has been unlawful including in breach of the lawfulness requirement; or (f) required to comply with a legal obligation.

GDPR	The 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.

Section 26: A data subject has a right – (a) to be informed of the use to which their personal data is to be put;
(b) to access their personal data in custody of data controller or data processor;
(c) to object to the processing of all or part of their personal data;
(d) to correct false or misleading data; and
(e) to delete false or misleading data about them.

Section 29: A data controller or data processor shall, before collecting personal data, in so far as practicable, inform the data subject of the rights of data subject specified under Section 26.

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 explicitly refer to this topic.

Section 12(5) of the Draft General Regulations: A compliance with a request for erasure shall be free of charge.

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.

Section 40(1)(b): A data subject may request a data controller or data processor to erase or destroy without undue delay personal data that the data controller or data processor is no longer authorised to retain, irrelevant, excessive or obtained unlawfully.

Section 12(3) of the Draft General Regulations: A data controller or data processor shall respond to a request for erasure within 14 days of the request.

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.

Section 40(3): Where a data controller or data processor is required to rectify or erase personal data under sub-section (1), but the personal data is required for the purposes of evidence, the data controller or data processor shall, instead of erasing or rectifying, restrict its processing and inform the data subject within a reasonable time.

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 40(2)(b): Where the data controller has shared the personal data with a third party for processing purposes, the data controller or data processor shall take all reasonable steps to inform third parties processing such data, that the data subject has requested the erasure or destruction of such personal data that the data controller is no longer authorised to retain, irrelevant, excessive or obtained unlawfully.

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 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

Section 40(3): Where a data controller or data processor is required to rectify or erase personal data under sub-section (1), but the personal data is required for the purposes of evidence, the data controller or data processor shall, instead of erasing or rectifying, restrict its processing and inform the data subject within a reasonable time.

Section 12(4) of the Draft General Regulations: A right of erasure does not apply if processing is necessary for one of the following reasons –

(a) to exercise the right of freedom of expression and information;

(b) to comply with a legal obligation;
(c) for the performance of a task carried out in the public interest or in the exercise of official authority;

(d) for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or

(e) for the establishment, exercise or defence of a legal claim.

GDPR	The Act

Exceptions (cont'd)

(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

The GDPR and the Act provide generally similar requirements for providing specific information to a data subject when collecting data. However, the Act is less explicit in terms of format and intelligibility requirements.

GDPR	The 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;

Section 26: A data controller or data processor shall, before collecting personal data, in so far as practicable, inform the data subject of -

(a) the rights of data subject specified under Section 26;

(b) the fact that personal data is being collected;

(c) the purpose for which the personal data is being collected;

(d) the third parties whose personal data has been or will be transferred to, including details of safeguards adopted;

(e) the contacts of the data controller or data processor and on whether any other entity may receive the collected personal data;

(f) a description of the technical and organizational security measures taken to ensure the integrity and confidentiality of the data;

(g) the data being collected pursuant to any law and whether such collection is voluntary or mandatory; and

(h) the consequences if any, where the data subject fails to provide all or any part of the requested data.

Section 4(1) of the Draft General Regulations: Subject to section 32 of the Act, a data controller or data processor shall, before processing personal data, inform the data subject —

(a) the nature of personal data to be processed;

(b) the scope of personal data to be processed;

GDPR	The Act

Informed prior to/ at collection (cont'd)

(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 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.

(c) the reasons for processing the required personal data; and (d) whether the personal data processed shall be shared with third parties.

[Note: Section 4(2), (3), and (7) of the Draft General Regulations provide further details on the manner of informing data subjects of the above.]

What information is to be provided

See Article 13(1) and (2) above.

See Section 26 of the Act above.

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.

Whilst the Act does not explicitly provide for notification requirements when data is collected from a third party, Section 28 provides: (1) A data controller or data processor shall collect personal data directly from the data subject.

(2) Despite sub-section (1), personal data may be collected indirectly where -

(a) the data is contained in a public record;

(b) the data subject has deliberately made the data public;

GDPR	The Act

When data is from third party

(c) the data subject has consented to the collection from another source;

(d) the data subject has an incapacity, the guardian appointed has consented to the collection from another source;

(e) the collection from another source would not prejudice the interests of the data subject;

(f) collection of data from another source is necessary -

(i) for the prevention, detection, investigation, prosecution and punishment of crime;

(ii) for the enforcement of a law which imposes a pecuniary penalty; or

(iii) for the protection of the interests of the data subject or another person.

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.

The Act does not explicitly refer to intelligibility requirements.

Format

See Article 12(1) above.

The Act does not explicitly refer to format requirements.

GDPR	The Act
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 (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.	The Act does not explicitly refer to particular exceptions.

Fairly consistent

5.3. Right to object

The Act provides a more general concept of the right to object than the GDPR and does not specify associated requirements such as fees and timeframes. Like the GDPR, however, the Act also establishes obligations regarding restricting processing.

Notably, the Draft General Regulation provides some further detail with regards to the right to object.

GDPR	The 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 26: A data subject has a right - [...] (c) to object to the processing of all or part of their personal data. Section 36: A data subject has a right to object to the processing of their personal data, unless the data controller or data processor demonstrates compelling legitimate interest for the processing which overrides the data subject's interests, or for the establishment, exercise or defence of a legal claim. Section 8(1) of the Draft General Regulations: Pursuant to Section 36 of the Act, a data subject may, where a specified processing may result in an unwarranted interference with their interests or rights, object to such processing by requesting a data controller or data processor not to process their personal data generally, for specified purpose or in a specified manner. Section 8(4) of the Draft General Regulations: The right to object applies as an absolute right where the processing of personal data is for direct marketing purposes which includes profiling to the extent that it is related to such direct marketing.
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.	Section 32(2): Unless otherwise provided under this Act, a data subject shall have the right to withdraw consent at any time.
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:	Section 34: (1) A data controller or data processor shall, at the request of a data subject, restrict the processing of personal data where -

GDPR	The Act

Restrict processing (cont'd)

(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.

(a) accuracy of the personal data is contested by the data subject, for a period enabling the data controller to verify the accuracy of the data;
(b) personal data is no longer required for the purpose of the processing, unless the data controller or data processor requires the personal data for the establishment, exercise or defence of a legal claim;
(c) processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or
(d) data subject has objected to the processing, pending verification as to whether the legitimate interests of the data controller or data processor overrides those of the data subject.
Section 7(3) of the Draft General Regulations: A data controller or data processor shall upon receiving the request —
(a) consider the restriction request;
(b) respond, in writing, to the data subject within fourteen days from the date of receiving the request;
(c) indicate on its system that the processing of personal data has been restricted; and
(d) notify any relevant third party where personal data subject to such restriction may have been shared.
Section 7(4) of the Draft General Regulations: A data controller or a data processor may implement a restriction to processing request by —
(a) temporarily moving the personal data to another processing system;
(b) making the personal data unavailable to third parties; or
(c) temporarily removing published data from a website or other public medium.
Section 7(5) of the Draft General Regulations: Where a data controller or data processor declines to comply with a request for restriction in processing, it shall within seven days notify the data subject of such decline giving reasons for the decision.

GDPR	The Act

Object to direct marketing

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.

[See Section 36 of the Act above on a general right to object]

Section 37: (1) A person shall not use, for commercial purposes, personal data obtained pursuant to the provisions of this Act unless the person - (a) has sought and obtained express consent from a data subject; or (b) is authorised to do so under any written law and the data subject has been informed of such use when collecting the data from the data subject.

(2) A data controller or data processor that uses personal data for commercial purposes shall, where possible, anonymise the data in such a manner as to ensure that the data subject is no longer identifiable.

(3) The Cabinet Secretary, in consultation with the Data Commissioner, may prescribe practice guidelines for commercial use of personal data in accordance with this Act.

Section 8(4) of the Draft General Regulations: The right to object to processing applies —

(a) as an absolute right where the processing of personal data is for direct marketing purposes; [...].

[Note: Section 18 of the Draft General Regulations provides further details on the right to object to direct marketing.]

Inform data subject of right

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 29: A data controller or data processor shall, before collecting personal data, in so far as practicable, inform the data subject of - (a) the rights of data subject specified under Section 26.

GDPR	The Act
Fees	
See Article 12(5) in section 5.1. above.	The Act does not explicitly address this topic. Section 8(6) of the Draft General Regulations: A data controller or data processor shall, without charging any fee, comply with a request to object processing within fourteen days of the receipt of the request.
Response timeframe	
See Article 12(3) in section 5.1. above.	The Act does not explicitly address this topic. Section 8(6) of the Draft General Regulations: A data controller or data processor shall, without charging any fee, comply with a request to object processing within fourteen days of the receipt of the request.
Format of response	
See Article 12(1) in section 5.1. above.	The Act does not explicitly address this topic.
Exceptions	
See Article 12(5) in section 5.1. above.	The Act does not specific exceptions for the right to object. Section 8(5) of the Draft General Regulations: Where the right to object is not absolute in circumstances contemplated under paragraph (4)(b), the data subject shall demonstrate — (a) compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or (b) the processing is for the establishment, exercise or defence of a legal claim.

Fairly inconsistent

5.4. Right of access

While the Act establishes a right of access in Section 26, it does not provide further requirements or clarify the processes for exercising this right.

Notably, the Draft General Regulation provides some further detail with regards to the right of access.

GDPR	The 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 26: A data subject has a right - [...] to access their personal data in custody of data controller or data processor.
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; (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;	The Act does not explicitly refer to the information that can be accessed. Section 9(1) of the Draft General Regulations: A data subject has a right to obtain from the data controller or data processor confirmation as to whether or not personal data concerning them is being processed, and where that is the case, access to the personal data and the information as to - (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, including recipients in other countries or territories; (d) where possible, the envisaged period for which the personal data may be stored, or, if not possible, the criteria used to determine that period; and (e) where the personal data is not collected from the data subject, any available information as to the source of collection.

GDPR	The Act

Information to be accessed (cont'd)

(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 29: A data controller or data processor shall, before collecting personal data, in so far as practicable, inform the data subject of - (a) the rights of data subject specified under Section 26.

Fees

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

The Act does not explicitly refer to fees for access.

Section 9(6) of the Draft General Regulations: A compliance with a request for access to personal data shall be free of charge.

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.

The Act does not explicitly refer to identity verification for general access. See Section 33 above in regard to age verification for children's data.

GDPR	The Act

Response timeframe

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

The Act does not explicitly refer to this topic.

Section 9(4) of the Draft General Regulations: A data controller or a data processor shall comply with a request by a data subject to access their personal data within seven days of the of the request.

Format of response

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

The Act does not explicitly refer to this topic.

Section 9(5) of the Draft General Regulations: Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

Exceptions

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

The Act does not explicitly refer to exceptions to the right to access.

5.5. Right not to be subject to discrimination

Consistent

The GDPR and the Act provide similarly for the regulation of automated processing by stipulating that data subjects have a right not to be subject to decisions made solely through automated processing which significantly affects the data subject.

GDPR	The Act

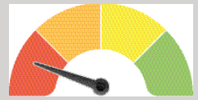
Definition of right

GDPR	The Act
The GDPR only implies this right and does not provide an explicit definition for it.	The Act only implies this right and does not provide an explicit definition for it.

Automated processing

GDPR	The Act
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]	Article 35(1): Every data subject has a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affects the data subject. [Article 35 goes on to detail this right, including exceptions]

5.6. Right to data portability



Inconsistent

The Act establishes a right to data portability with many similarities to the GDPR. A primary difference is that the Act frames this right in broader terms.

Notably, the Draft General Regulation provides some further detail with regards to the right to data portability.

GDPR	The Act

Grounds for portability

GDPR	The Act
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.	Section 38: (1) A data subject has the right to receive personal data concerning them in a structured, commonly used and machine-readable format. (2) A data subject has the right to transmit the data obtained under sub-section (1), to another data controller or data processor without any hindrance. Section 12(1) of the Draft General Regulations: Pursuant to Section 38 of the Act, a data subject may apply to port or copy their personal data from one data controller or data processor to another.

Inform data subject of right

GDPR	The Act
See Article 12(1) in section 5.1.	The Act does not explicitly refer to informing data subjects about their right to data portability.

Fees

GDPR	The Act
See Article 12(5) in section 5.1. above.	Section 38(6): A data controller or data processor shall comply with data portability requests, at reasonable cost and within a period of thirty days. Section 11(4) of the Draft General Regulations: Where a fee is charged under paragraph (2), the fee shall be reasonable and not exceed the actual cost incurred to actualise the request.

Response timeframe

GDPR	The Act
See Article 12(3) in section 5.1. above.	Section 38(6): A data controller or data processor shall comply with data portability requests, at reasonable cost and within a period of thirty days.

GDPR	The Act
Response timeframe	
See Article 12(3) in section 5.1. above.	Section 11(3) of the Draft General Regulations: The data controller or data processor shall within thirty days from the date of receipt of the request and upon payment of any charge port personal data to the data subject's choice of recipient. Section 11(6) of the Draft General Regulations: Where a data controller or data processor declines the portability request, it shall within seven days notify, in writing, the data subject of the decision and the reasons for such decline in writing.
Format	
See Article 20(1) above.	See Section 38(1) of the Act above.
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.	Section 38(3): Where technically possible, the data subject shall have the right to have the personal data transmitted directly from one data controller or processor to another.
Technically feasible	
See Article 20(2) above.	See Section 38(3) of the Act above.
Exceptions	
See Article 12(5) in section 5.1. above.	Section 38(7): Where the portability request is complex or numerous, the period under sub-section (6) may be extended for a further period as may be determined in consultation with the Data Commissioner. Section 11(7) of the Draft General Regulations: The exercise of the right to data portability by a data subject shall not negate the rights of a data subject provided under the Act.

6. Enforcement

6.1. Monetary penalties

There are several similarities between the GDPR and the Act, including the provisions of monetary penalties and the types of mitigating factors that can be taken into account. However, key differences between the pieces of legislation are that the Act provides for potential prison terms, that individuals may be held liable for offences, and that the amount of fines that may be issued differ.

GDPR	The 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.	Sections 61 and 63 provide that the Data Protection Commissioner has the power to issue fines.
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; (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).	Section 61: A person who, in relation to the exercise of a power conferred by Section 9 - (a) obstructs or impedes the Data Commissioner in the exercise of their powers; (b) fails to provide assistance or information requested by the Data Commissioner; (c) refuses to allow the Data Commissioner to enter any premises or to take any person with them in the exercise of their functions; (d) gives to the Data Commissioner any information which is false or misleading in any material aspect, commits an offence and is liable on conviction to a fine not exceeding 5,000,000 shillings [approx. €38,000], or to imprisonment for a term not exceeding two years, or to both. Section 63: In relation to an infringement of a provision of this Act, the maximum amount of the penalty that may be

GDPR	The Act

Fine maximum (cont'd)

(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.

imposed by the Data Commissioner in a penalty notice is up to 5,000,000 shillings [approx. €38,000], or in the case of an undertaking, up to 1% of its annual turnover of the preceding financial year, whichever is lower.

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.

Under Section 63, in the case of an undertaking, fines may be issued that equate to up to 1% of its annual turnover of the preceding financial year.

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 62(2): In deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Data Commissioner shall, so far as relevant, have regard -

(a) to the nature, gravity and duration of the failure;

(b) to the intentional or negligent character of the failure;

(c) to any action taken by the data controller or data processor to mitigate the damage or distress suffered by data subjects;

(d) to the degree of responsibility of the data controller or data processor, taking into account technical and organisational measures;

(e) to any relevant previous failures by the data controller or data processor; to the degree of co-operation with the Data Commissioner, in order to remedy the failure and mitigate the possible adverse effects of the failure;

(g) to the categories of personal data affected by the failure;

(h) to the manner in which the infringement became known to the Data Commissioner, including whether, and if so to what extent, the data controller or data processor notified the Data Commissioner of the failure;

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.

Section 58(3): Any person who, without reasonable excuse, fails to comply with an enforcement notice commits an offence and is liable on conviction to a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years, or to both.

Section 61: A person who, in relation to the exercise of a power conferred by section 9 -

(a) obstructs or impedes the Data Commissioner in the exercise of their powers;

(b) fails to provide assistance or information requested by the Data Commissioner;

(c) refuses to allow the Data Commissioner to enter any premises or to take any person with them in the exercise of their functions;

(d) gives to the Data Commissioner any information which is false or misleading in any material aspect, commits an offence and is liable on conviction to a fine

GDPR	The Act
Imprisonment	
	Section 73: A person who commits an offence under this Act for which no specific penalty is provided or who otherwise contravenes this Act shall, on conviction, be liable to a fine not exceeding three million shillings or to an imprisonment term not exceeding ten years, or to both.
DPO liability	
Not applicable.	See above for liability of persons.

6.2. Supervisory authority

The scope, general powers, and tasks assigned to data protection authorities under the GDPR and the Act are largely similar. There is, however, a significant difference in the level of detail provided to describe and regulate these powers.

GDPR	The 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 5(1): There is established the office of the Data Protection Commissioner which shall be a body corporate with perpetual succession and a common seal.
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.	Section 9: The Data Commissioner shall have power to - (a) conduct investigations on own initiative, or on the basis of a complaint made by a data subject or a third party; (b) obtain professional assistance, consultancy or advice from such persons or organisations whether within or outside public service as considered appropriate; (c) facilitate conciliation, mediation and negotiation on disputes arising from this Act; (d) issue summons to a witness for the purposes of investigation; (e) require any person that is subject to this Act to provide explanations, information and assistance in person and in writing; (f) impose administrative fines for failures to comply with this Act; (g) undertake any activity necessary for the fulfilment of any of the functions of the Office; and (h) exercise any powers prescribed by any other legislation. Part II of the Draft Enforcement Regulations further outlines the procedure for handling complaints.

GDPR	The Act

Corrective powers

GDPR	The Act
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;	Under Sections 9, 58, 62, 63, and 66, the Data Protection Commissioner has the power to: (a) issue enforcement notices; (b) issue penalty notices; (c) administrative fines; and (d) apply for a preservation order. Part III of the Draft Enforcement Regulations specifies the requirements for issuing enforcement notices.

GDPR	The Act

Corrective powers (cont'd)

GDPR	The Act
(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.	

Authorisation/ advisory powers

GDPR	The Act
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.	Section 9: The Data Commissioner shall have power to - [...] (b) obtain professional assistance, consultancy or advice from such persons or organisations whether within or outside public service as considered appropriate; (c) facilitate conciliation, mediation and negotiation on disputes arising from this Act; [...] (e) require any person that is subject to this Act to provide explanations, information and assistance in person and in writing; [...] (g) undertake any activity necessary for the fulfilment of any of the functions of the Office; and (h) exercise any powers prescribed by any other legislation.

GDPR	The Act

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;

(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

Section 8: The Office shall -

(a) oversee the implementation of and be responsible for the enforcement of this Act;

(b) establish and maintain a register of data controllers and data processors;

(c) exercise oversight on data processing operations, either of own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with this Act;

(d) promote self-regulation among data controllers and data processors;

(e) conduct an assessment, on its own initiative of a public or private body, or at the request of a private or public body for the purpose of ascertaining whether information is processed according to the provisions of this Act or any other relevant law;

(f) receive and investigate any complaint by any person on infringements of the rights under this Act;

(g) take such measures as may be necessary to bring the provisions of this Act to the knowledge of the general public;

(h) carry out inspections of public and private entities with a view to evaluating the processing of personal data;

(i) promote international cooperation in matters relating to data protection and ensure country's compliance on data protection obligations under international conventions and agreements;

(j) undertake research on developments in data processing of personal data and ensure that there is no significant risk or adverse effect of any developments on the privacy of individuals; and

(k) perform such other functions as may be prescribed by any other law or as necessary for the promotion of object of this Act.

GDPR	The Act

Tasks of authority (cont'd)

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;

(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

(2) The Office of the Data Commissioner may, in the performance of its functions collaborate with the national security organs.

(3) The Data Commissioner shall act independently in exercise of powers and carrying out of functions under this Act.

GDPR	The Act

Tasks of authority (cont'd)

(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 70: The Data Commissioner shall, within three months after the end of each financial year, prepare and submit to the Cabinet Secretary a report of the operations of the Office for the immediately preceding year.

6.3. Civil remedies for individuals

Fairly consistent

Both the GDPR and the Act provide for data subjects to seek compensation or judicial remedy if they have suffered material or non-material damage. Similarly, both legislative frameworks establish that data processors may be held liable under certain circumstances and do not specify an amount for damages. The GDPR and the Act differ, though, in relation to the capacity to mandate another body to act as representative for the data subject.

GDPR	The 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 56: A data subject who is aggrieved by a decision of any person under this Act may lodge a complaint with the Data Commissioner in accordance with this Act.

Section 65: A person who suffers damage by reason of a contravention of a requirement of this Act is entitled to compensation for that damage from the data controller or the data processor.

Section 58 of the Draft General Regulations: A person aggrieved by any decision under the Regulation or noncompliance with any with any provision may lodge a complaint with the Data Commissioner in accordance with the Act and the Regulations made thereunder.

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.

Section 65(4): 'damage' includes financial loss and damage not involving financial loss, including distress.

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 explicitly refer to mandates for representation.

GDPR	The Act
Specifies amount for damages	
Not applicable.	Not applicable.
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.	Section 65(2): Subject to subsection (1) - (a) a data controller involved in processing of personal data is liable for any damage caused by the processing; and (b) a data processor involved in processing of personal data is liable for damage caused by the processing only if the processor - (i) has not complied with an obligation under the Act specifically directed at data processors; or (ii) has acted outside, or contrary to, the data controller's lawful instructions.
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.	Section 65(3): A data controller or data processor is not liable in the manner specified in subsection (2) if the data controller or data processor proves that they are not in any way responsible for the event giving rise to the damage.