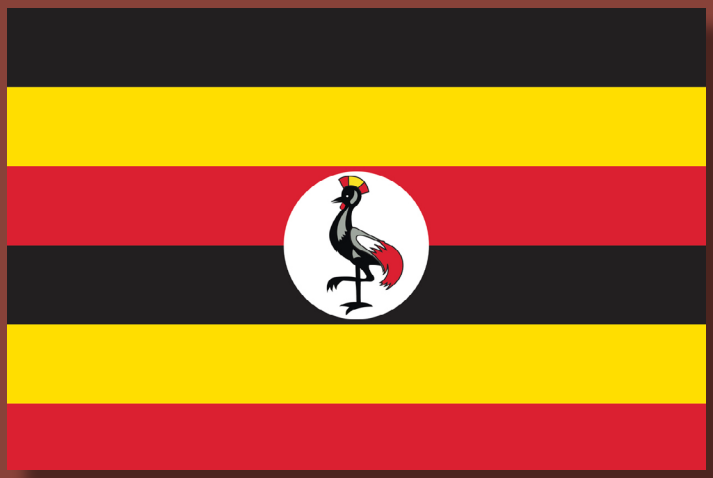


Comparing privacy laws:
GDPR v. Data Protection and Privacy Act

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

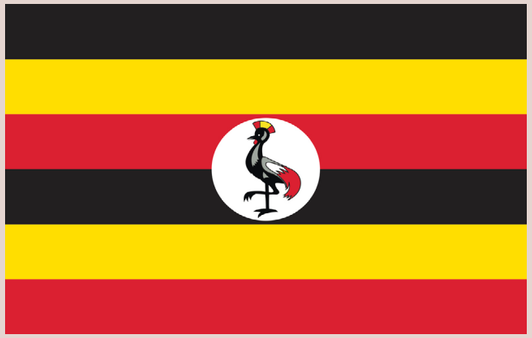
OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

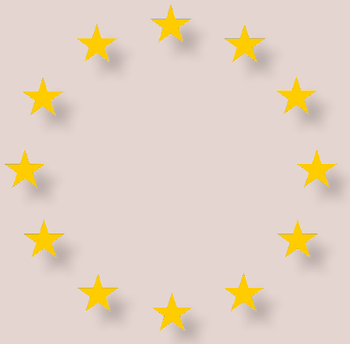
The OneTrust DataGuidance™ platform includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Cross-Border Charts which allow you to compare regulations across multiple jurisdictions at a glance, a daily customised news service and expert analysis.

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 and Privacy Act 2019 ('the Act'), which came into force in May 2019, is the primary piece of data protection legislation in Uganda and has been supplemented with the Data Protection and Privacy Regulations, 2021 ('the Regulations'), which were introduced on 12 March 2021.

The Act and Regulations share several similarities with the GDPR in terms of overarching principles and the general regulation of data controllers, processors, and data subject rights. Furthermore, similar to the requirement under the GDPR to provide for a data protection authority responsible for monitoring the application of the GDPR, the Regulations provide for the establishment of the Personal Data Protection Office ('PDPO') within the National Information Technology Authority - Uganda ('NITA-U'), with the PDPO responsible for the overall implementation of the Act and the Regulations.

However, there are also significant differences between the frameworks, particularly in relation to the obligations of organisations. Notably, the Regulations have introduced additional provisions, particularly in relation to data processing records, Data Protection Impact Assessments ('DPIA'), data protection officer ('DPO') appointment, and data transfers. However, in general terms, the provisions within the Act and its Regulations are slightly less detailed than those found within the GDPR.

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

Structure and overview of the Guide

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

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

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

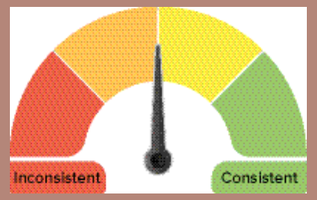
Key for giving the consistency rate

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

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

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

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



Usage of the Guide

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

1. Scope

Fairly consistent

1.1. Personal scope

The Act employs similar core concepts as the GDPR and refers to data controllers, data processors, and data subjects. The GDPR and the Act differ, however, in that the latter does not explicitly exclude deceased persons' data. In addition, unlike the GDPR, the Act includes a definition for data collectors.

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 person who alone, jointly with other persons or in common with other persons or as a statutory duty determines the purposes for and the manner in which personal data is processed or is to be processed.
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 person other than an employee of the data controller who processes the 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 individual from whom or in respect of whom personal information has been requested, collected, collated, processed or stored.
Public bodies	
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body.	Section 2: 'public body' includes the Government, a department, service or undertaking of the Government, Cabinet, Parliament, a court, local Government administration or a local council and any committee or commission thereof, an urban authority, a municipal council and any committee of any such council, any corporation, committee, board, commission or similar body whether corporate or incorporate

GDPR	The Act
Public bodies (cont'd)	
	Sestablished by an Act of Parliament relating to undertakings of public services or such purpose for the benefit of the public or any section of the public to administer funds or property belonging to or granted by the Government or money raised by public subscription, rates, taxes, cess or charges in pursuance of any written law and any council, board, committee or society established by an Act of Parliament for the benefit, regulation and control of any profession.
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 1: The Act applies to a person, institution or public body collecting, processing, holding or using personal data within Uganda; and outside Uganda who collects, processes, holds, or uses personal data relating to Ugandan citizens.
Place of residence	
See Recital 14, above.	See Section 1 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.	Section 2: The Act's definition of 'personal data' does not distinguish between information about a living or deceased person. h.

1.2. Territorial scope

Like the GDPR, the Act applies extraterritorially. However, the Act does not explicitly regulate goods and services or monitoring from abroad.

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 1: The Act applies to a person, institution or public body collecting, processing, holding or using personal data within Uganda; and outside Uganda who collects, processes, holds, or uses personal data relating to Ugandan citizens. Section 30 of the Regulations addresses the requirements for processing personal data outside of Uganda.
Extraterritorial	
See Article 3, above.	See Section 1 of the Act above.
Goods & servicies from abroad	
Recital 23: In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.	The Act does not refer to goods and services from abroad.
Monitoring from abroad	
Recital 24: The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.	The Act does not refer to monitoring from abroad.

1.3. Material scope

Fairly consistent

The Act and the GDPR provide similar definitions of personal data and data processing, and both include specific requirements for special categories of, or sensitive, data. The two pieces of legislation differ, however, in terms of the general exemptions they stipulate, and in regard to anonymised and pseudonymised 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 information about a person from which the person can be identified, that is recorded in any form and includes data that relates to:

a) the nationality, age or marital status of the person;

b) the educational level, or occupation of the person;

c) an identification number, symbol or other particulars assigned to a person;

d) identity data; or

e) other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual.

Data processing

Article 4(2): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Section 2: 'processing' means any operation which is performed upon collected data by automated means or otherwise including:

a) organisation, adaptation or alteration of the information or data;

b) retrieval, consultation or use of the information or data;

c) disclosure of the information or data by transmission, dissemination or otherwise making available; or

d) alignment, combination, blocking, erasure or destruction of the information or data.

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 9(1): 'Special personal data' is referred to as personal data which relates to the religious or philosophical beliefs, political opinions, sexual life, financial information, health status or medical records of an individual.

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 18(4): A data controller shall destroy or delete a record of personal data or de-identify the record at the expiry of the retention period.

Section 18(5): The destruction or deletion of a record of personal data shall be done in a manner that prevents its reconstruction in an intelligible form.

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.

See Section 18(4)-(5) of the Act above.

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 2: 'processing' means any operation which is performed upon collected data by automated means or otherwise.

GDPR	The Act

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 9(2): The collection of and processing of special personal data does not apply to information collected under the Uganda Bureau of Statistics Act 1998.

2. Key definitions

Fairly consistent

2.1. Personal data

The GDPR and the Act set out similar understandings for the concepts of personal data and special categories of 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 information about a person from which the person can be identified, that is recorded in any form and includes data that relates to:

a) the nationality, age or marital status of the person;

b) the educational level, or occupation of the person;

c) an identification number, symbol or other particulars assigned to a person;

d) identity data; or

e) other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual.

Special categories of data

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

Section 9(1): 'Special personal data' is referred to as personal data which relates to the religious or philosophical beliefs, political opinions, sexual life, financial information, health status or medical records of an individual.

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.

The Act does not specifically refer to online identifiers.

GDPR	The Act
Data Collector	
The GDPR does not provide for a definition of 'data collector'.	Section 2: 'data collector' means a person who collects personal data.
Recipient	
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: 'recipient' means a person to whom data is disclosed including an employee or agent of the data controller or the data processor to whom data is disclosed in the course of processing the data for the data controller, but does not include a person to whom disclosure is made with respect to a particular inquiry pursuant to an enactment.
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' in relation to personal data, means a person other than the data subject, the data collector, data controller, or any data processor or other person authorised to process data for the data controller or processor.

2.2. Pseudonymisation

Unlike the GDPR, the Act does not directly refer to anonymisation and pseudonymisation, however it does contain relevant provisions related to the destruction and de-identification of data.

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.	The Act does not specifically define anonymised data. However, it refers to de-identified data. Section 18(4): A data controller shall destroy or delete a record of personal data or de-identify the record at the expiry of the retention period. Section 18(5): The destruction or deletion of a record of personal data shall be done in a manner that prevents its reconstruction in an intelligible form.
Pseudonymisation	
Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	The Act does not explicitly refer to pseudonymisation.

2.3. Controllers and processors

The Act and the GDPR provide similar definitions for data controllers and data processors, as well as requirements for agreements between these parties as well as obligations to appoint a DPO. Furthermore, while the Act itself does not specifically address DPIAs, the Regulations outline when a DPIA should be conducted and what it should include, akin to the relevant provisions of the GDPR.

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 person who alone, jointly with other persons or in common with other persons or as a statutory duty determines the purposes for and the manner in which personal data is processed or is to be processed.

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 person other than an employee of the data controller who processes the 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 21(2): A contract between a data controller and a data processor relating to processing of personal data, shall require the data processor to establish and maintain the confidentiality and security measures necessary to protect the integrity of the personal data.

GDPR	The Act

Data Protection Impact Assessment ('DPIA')

DPIA is not specifically defined, however Article 35 sets out requirements for DPIAs (see section 5.3. for further information).

Section 12 of the Regulations: Where the collection or processing of personal data poses a high risk to the rights and freedoms of natural persons, the data collector, data processor or data controller must, prior to the collection or processing, carry out an assessment of the impact of the envisaged collection or processing operations on the protection of personal data. Every DPIA must include a systematic description of the envisaged processing and the purposes of the processing, an assessment of the risks to personal data and the measures to address the risks, and any other matters the PDPO may require (see section 4.3. for further information).

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 6 mandates the designation of a DPO.

Section 47 of the Regulations addresses the specifics of designating a DPO (see section 4.4. for further information).

2.4. Children

Fairly consistent

Like the GDPR, the Act provides additional requirements for children's data. However, unlike the GDPR, the Act does not contain requirements for the provision of privacy notices to children.

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 8 provides: A person shall not collect or process personal data relating to a child unless the collection or processing thereof is:

a) carried out with the prior consent of the parent or guardian or any other person having authority to make decisions on behalf of the child;

b) necessary to comply with the law; or

c) for research or statistical purposes.

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.

See Section 8 of the Act above.

Section 11 of the Regulations: For the purposes of Section 8 of the Act, every data collector, controller, processor must establish a system to ascertain the age of persons whose personal data is to be collected, processed, or stored, and where the data relates to a child, the manner of obtaining the consent of a parent or legal guardian.

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 specifically address privacy notices for children.

2.5. Research

Fairly inconsistent

Like the GDPR, the Act provides exemptions for processing for scientific or historical research purposes in certain instances. However, the Act does not establish requirements for appropriate safeguards in the manner of the GDPR, nor does it provide specific data subject rights in the context of scientific or historical research.

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.

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

Compatibility with original purpose of collection

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

Section 17(3)(e): The further processing of data is considered to be compatible with the purpose of collection where the data is used for historical, statistical or research purposes and the person responsible for the processing ensures that:

i) the further processing is carried out solely for the purpose for which the data was collected; and

ii) that the data is not published in a form likely to reveal the identity of the data subject.

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

The Act does not provide for appropriate safeguards. However, Section 18(2)(f) states that retention of personal data provisions do not apply to personal data retained for historical, statistical, or research purposes.

GDPR	The Act

Appropriate safeguards (cont'd)

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

Data subject rights (research)

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

The Act does not refer to data subject rights in the context of scientific or historical research.

3. Legal basis

Fairly consistent

The Act sets out very similar grounds for the processing of personal data to the GDPR, as well as comparable additional requirements for the processing of special categories of, or sensitive, data. Moreover, the Act has provisions defining conditions for consent, however it does not address matters such as processing for journalistic/artistic purposes.

GDPR	The Act

Legal grounds

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

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

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

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

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

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

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

Section 7(1): Subject to subsection (2), a person shall not collect or process personal data without the prior consent of the data subject.

(2) Personal data may be collected or processed:

a) where the collection or processing is authorised or required by law; or

b) where it is necessary:

i) for the proper performance of a public duty by a public body;

ii) for national security;

iii) for the prevention, detection, investigation, prosecution or punishment of an offence or breach of law.

c) 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;

d) for medical purposes; or

e) for compliance with a legal obligation to which the data controller is subject.

Sensitive data (legal basis)

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

There are specific requirements for processing special personal data under Section 9 of the Act.

GDPR	The Act

Conditions for consent

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

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

Section 7(3): Except for data collected or processed under subsection (2), where a data subject objects to the collection or processing of personal data, the person who is collecting or processing the personal data shall stop the collection or processing of the personal data.

Section 2: 'consent' means any freely given, specific, informed and unambiguous indication of the data subject's wish which he or she, by a statement or by a clear affirmative action, signifies agreement to the collection or processing of personal data relating to him or her.

Schedule 1 of the Regulations includes a form for notice of objection to the collection/processing of personal data.

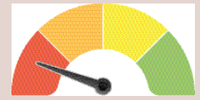
Journalism/ artistic purposes

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

The Act does not refer to journalism or artistic purposes.

4. Controller and processor obligations

4.1. Data transfers



Inconsistent

The Act provides for a similar notion of adequate protection as the GDPR. However, the Act only recognises consent as an alternative mechanism for data transfers, whereas the GDPR provides that transfers to third country or an international organisation may still occur if appropriate safeguards are provided.

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 19: Where a data processor or data controller based in Uganda processes or stores personal data outside Uganda, the data processor or data controller shall ensure that:

a) the country in which the data is processed or stored has adequate measures in place for the protection of personal data at least equivalent to the protection provided for by this Act; or

b) the data subject has consented.

Section 30(1) of the Regulations: A data collector, data processor or data controller shall not process or store personal data outside Uganda unless the data collector, processor, or controller demonstrates to the PDPO (a) the country outside Uganda where the personal data is to be processed or stored has adequate measures in place for the protection of the personal data at least equivalent to the protection provided for by the Act; or (b) the data subject has consented to the processing. (5) Where the data collector, processor, or controller wishes to process or store personal data in a country that does not appear on the list of countries deemed adequate by the PDPO, it is the responsibility of the collector, processor, or controller to prove that the country has adequate measures in place for the protection of personal data, at least equivalent to the protection provided by the Act.

GDPR	The Act

Other mechanisms for data transfers

Article 46(1): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

(2) The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) binding corporate rules in accordance with Article 47;

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

(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

GDPR	The Act

Other mechanisms for data transfers (cont'd)

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

Data localisation

Not applicable.	Not applicable.

4.2. Data processing records

Fairly Inconsistent

While the GDPR requires both data controllers and data processors to maintain data processing records, the Act does not specify equivalent obligations for either. However, the Act does set out general provisions for registering with the PDPO.

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 provide for a requirement to maintain data processing records. However, Section 29 provides: the PDPO shall keep and maintain a data protection register and an application by a data controller or other person to register shall be made in the prescribed manner. Section 29(1) of the Act: The PDPO shall keep and maintain a data protection register. (2) The PDPO shall register in the data protection register, every person, institution or public body collecting or processing personal data and the purpose for which the personal data is collected or processed. (3) An application by a data controller or other person to register shall be made in the prescribed manner. Article 30: The PDPO shall make the information contained in the Data Protection Register available for inspection by any person. Section 14(1): The Regulations provide the register shall contain information relating to data collectors, data processors and data controllers including the purpose for which personal data is collected. (2) The Register will contain the following information (a) the name of the person, institution, or body (b) the address of the person, institution or public body (c) the nature of the personal data being collected or processed by the person, institution or public body; and (e) the purpose for the collection or processing of personal data.

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).	See Section 29 of the Act above.
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 provide for such requirements.
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.	The Act does not provide for such requirements.

GDPR	The Act

Exemptions

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

General Data Processing Notification ('DPN')

Not applicable.	Section 15(1) of the Regulations: Subject to subregulation (2), every data collector, data processor or data controller shall register with the PDPO. (2) The PDPO shall, in consultation with the Board, by notice in the Gazette, exempt certain data collectors, data processors or data controllers from the requirement to register with the PDPO. Section 16(1) of the Regulations: An application for registration shall be in Form 2 in Schedule 1 and shall be accompanied by the fee specified in Schedule 2. Furthermore, Section 16(2) of the Regulations outlines what should be included within the application. (3) Every application shall be accompanied by a written undertaking by the applicant not to process or store personal data in a country outside Uganda unless such country has adequate measures in place, at least equivalent to the protection provided for by the Act for the protection of the personal data and the data subject consents to the transfer.

4.3. Data protection impact assessment

Although the Act itself does not provide requirements on DPIAs, the Regulations, along with the GDPR, do provide for a requirement to carry out a DPIA prior to the processing of personal data, and outline the required contents of a DPIA.

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 12(1) of the Regulations: Where the collection or processing of personal data poses a high risk, data collectors, processors, and controllers must, prior to the collection or processing carry out an assessment of the impact of the envisaged collection or processing operations on the protection of personal data.

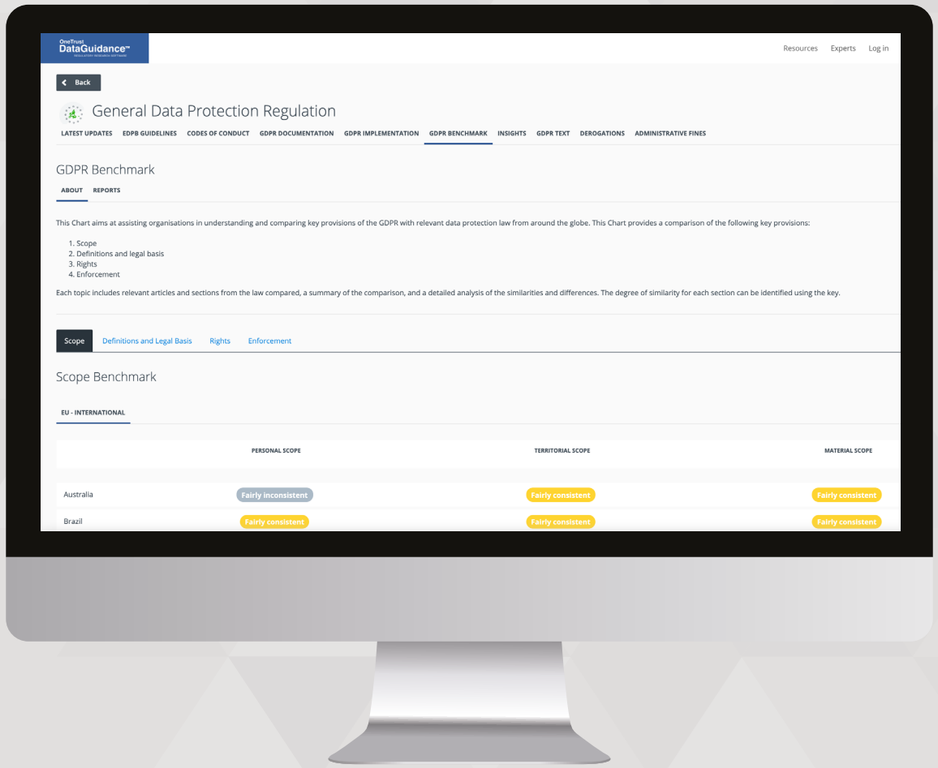
DPIA content requirements

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 12(2) of the Regulations: Every data protection impact assessment must include: - a systematic description of the envisaged processing and the purposes of the processing; - an assessment of the risks to personal data and the measures to address the risks; and - any other matter the PDPO may require.

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

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.

Consultation with authority

Article 36(1): The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. [Article 36 goes on to detail requirements related to such prior consultation].

The Act does not provide for requirements for DPIA consultation.

Section 12(3) of the Regulations: The PDPO shall establish and make a list of the processing operations which are subject to the requirement for a DPIA.

4.4. Data protection officer appointment

The Act provides for the requirement to appoint a DPO, while the Regulations provide further details and requirements regarding DPO tasks and relevant qualifications.

GDPR	The Act

DPO tasks

Article 39(1): The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority; and

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

Section 47(3): The Regulations provides the responsibilities of a data protection officer are (a) to conduct regular assessments and audits to ensure compliance with the Act (b) to serve as the point of contact between the person, institution or public body and the PDPO (c) to maintain records of all data processing activities conducted by person, institution or public body (d) to respond to data subjects and inform them about how their personal data is being used and what measures the person, institution or public body, has put in place to protect the data, and (e) to ensure that data subjects' requests to see copies of their personal data or have their personal data erased are fulfilled or responded to, as necessary.

When is a DPO required

Article 37(1): The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

Section 6: For purposes of this Act, and in so far as it applies to an institution, the head of the institution shall designate a person as the data protection officer responsible for ensuring compliance with this Act.

GDPR	The Act
When is a DPO required (cont'd)	
(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.	Section 47(2): The Regulations provide every person, institution or public body that processes or controls personal data shall designate a data protection officer where (a) the activities of the person, institution of public body consist of processing operations which by virtue of their nature, scope or purpose require regular and systematic monitoring of data subjects on a large scale; or (b) the core activities of the person, institution or public body consist of processing of special person data in accordance with the Act.
Group appointments	
Article 37(2): A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.	The Act does not provide for requirements in relation to group appointments.
Notification of DPO	
Article 37(7): The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.	The Act does not provide for notification requirements.
Qualifications	
Article 37(5): The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.	Section 47(4): The regulations provide every person, institution or public body that designates a data protection officer shall provide such data protection officer with the relevant training to enable them to perform the duties of a data protection officer.

4.5. Data security and data breaches

Fairly consistent

The GDPR, the Act, and the Regulations establish similar general data security provisions and require that authorities should be notified of data breaches within a specific timeframe. However, unlike the GDPR, the Act does not provide for specific exceptions to data breach notification. Furthermore, the Act provides the PDPO with the power to require that data subjects are notified of breaches, including through public announcements.

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 20(1): A data controller, data collector or data processor shall secure the integrity of personal data in the possession or control of a data controller, data processor or data collector by adopting appropriate, reasonable, technical and organisational measures to prevent loss, damage, or unauthorised destruction and unlawful access to or unauthorised processing of the personal data. (2) For the purposes of subsection (1), the data controller shall take measures to- (a) identify reasonably foreseeable internal and external risks to personal data under that person's possession or control; (b) establish and maintain appropriate safeguards against the identified risks; (c) regularly verify that the safeguards are effectively implemented; and (d) ensure that the safeguards are continually updated in response to new risks or deficiencies, (3) A data controller shall observe generally accepted information security practices and procedures, and specific industry or professional rules and regulations. Section 21(1): A data controller shall not permit a data processor to process personal data for the data controller, unless the data processor establishes and complies with the security measures specified under this Act. (2) A contract between a data controller and a data processor relating to processing of personal data, shall require the data processor to establish and maintain the confidentiality and security measures

GDPR	The Act

Security measures defined (cont'd)

necessary to protect the integrity of the personal data.
Section 31(1) of the Regulations: For the purposes of Section 20(3) of the Act, the Office shall publish, in the Gazette, the generally accepted information security practices and procedures and specific industry professional rules and regulations applicable to the security of personal data.

(2) Information security practices and procedures and specific industry professional rules and regulations applicable to the security of personal data referred to in subregulation (1) include:
- administrative measures, that is to say, measures aimed at creating efficient guidelines and security standards for dealing with personal data; and
- technical measures, that is to say, measures aimed at preventing overlap and restricting access to systems and personal data.

Section 32(1) of the Regulations: For the purposes of Section 21 of the Act, a data controller shall ensure that any data processor that processes personal data for the data controller develops and implements appropriate security measures to safeguard the personal data.

Data breach notification to authority

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

Section 23(1): Where a data collector, data processor or data controller, believes that the personal data of a data subject has been accessed or acquired by an unauthorised person, the data collector, data processor or data controller, shall immediately notify PDPO in the prescribed manner, of the unauthorised access or acquisition and the remedial action taken.
Section 33(1) of the Regulations: The notification required under Section 23(1) [of the Act] shall be made immediately after the occurance of the data breach.
Section 33(3) of the Regulations provides that the notification shall include (a) the nature of the personal data breach (b) the personal data which is the subject of the data breach (c) the categories and approximate number of data subjects affected by the personal data breach (d) the likely consequences of the personal data breach (e) the appropriate remedial measures taken or proposed to address the personal data breach, and (f) the name and contact details of the data protection officer or other point of contact.

GDPR	The Act

Timeframe for breach notification

See Article 33(1) above.

See Section 23(1) of the Act and Section 33(1) of the Regulations above.

Notifying data subjects of data breach

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

Section 23(2): The PDPO shall determine and notify the data controller, data collector or data processor whether the data controller, data collector or data processor should notify the data subject of the breach.
(3) Where the PDPO determines that the data collector, data processor or data controller should notify the data subject, the notification shall be made by-
(a) registered mail to the data subject's last known residential or postal address;
(b) electronic mail to the data subject's last known electronic mail address;
(c) placement in a prominent position on the website of the responsible party; or
(d) publication in the mass media.
(4) A notification referred to in sub section (3) shall provide sufficient information relating to the breach to allow the data subject to take protective measures against the consequences of unauthorised access or acquisition of the data.
(5) Where the PDPO has grounds to believe that publicity would protect a data subject who is affected by the unauthorised access or acquisition of data, the PDPO shall direct the responsible party to publicise in the specified manner, the fact of the compromise to the integrity or confidentiality of the personal data.
Section 33(4) of the Regulations: The PDPO shall, immediately after receiving a notification referred to in subregulation (1), provide the concerned data collector, data processor or data controller with appropriate guidance on how to deal with the data breach.
(5) The guidance referred to in subregulation (4) shall include:
(b) the manner of notification of the data subject affected by the data breach including requiring the data collector, data processor or data controller to provide the data subject with sufficient information relating to the data breach in order to allow the data subject to take protective measures against the consequences of the data breach; and

GDPR	The Act
Notifying data subjects of data breach (cont'd)	
	(c) any measures to alert the general public on the nature of the data breach.
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.	See Section 23(1) of the Act above.
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.	The Act does not explicitly provide relevant exceptions.

4.6. Accountability

Fairly inconsistent

Both the GDPR and the Act provide for a principle of accountability, however they do so in different forms with the Act emphasising the capacity for data subjects to hold persons to account. Furthermore, the Act does not establish a distinction like the GDPR between processor and controller 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.]	Section 3(1): A data collector, data processor or data controller or any person who collects, processes, holds or uses personal data shall- (a) be accountable to the data subject for data collected, processed held or used.
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.	In general terms, the Act does not differentiate liabilities between data controllers, collectors, or processors. 'Persons' may be held liable for offences under the Act.

5. Rights

5.1. Right to erasure

Unlike the GDPR, the Act only provides data subjects with the capacity to request the erasure of data in the context of correcting or deleting inaccurate data or information that is unlawfully obtained or held.

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 16(1): A data subject may request a data controller to-

(a) correct or delete personal data about the data subject held by or under the control of the data controller that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

(b) destroy or delete a record of personal data about the data subject held by the data controller which the controller no longer has the authority to retain.

Section 28(1): Where the PDPO is satisfied on a complaint of a data subject that personal data on that data subject is inaccurate, the PDPO may order the data controller to rectify, update, block, erase, or destroy the data.

(2) Subsection (1) applies whether the data is an accurate record of information received or obtained by the data controller from the data subject or a third party.

Schedule 1 Form 9 of the Regulations can be used when requesting erasure.

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 13(1)(1): A person collecting personal data shall inform the data subject about- [...] (h) the existence of the right of access to and the right to request rectification of the data collected before the collection.

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.

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 16(2): On receipt of the request, a data controller shall comply with the request.

Section 39(2) of the Regulations: Where the data controller does not comply with a request within 30 days of receipt of the request, the data subject may make a complaint to the PDPO.

GDPR	The Act

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 16(3): Where the data controller is not able to comply with the request under subsection (1), the data controller shall inform the data subject of the rejection, and the reasons for the rejection in writing.

[...] (5) The data controller shall notify the data subject of the action taken as a result of the request.

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 28(4): Where the data complained of has been rectified, blocked, updated, erased or destroyed, the data controller is required to notify third parties to whom the data has been previously disclosed of the rectification, blocking, updated, erasure or destruction.

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

The Act does not explicitly outline exceptions. However, Section 29(4) of the Regulations provides that where a data controller cannot comply with the request for erasure of personal data, the data controller shall, in writing, inform the data subject of the rejection, and any action taken as a result of the request.

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 inconsistent

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 13 provides that information is to be given to data subject before collection of data.

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.

What information is to be provided

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

Section 13(1): A person collecting personal data shall inform the data subject about:
(a) the nature and category of data being collected;
(b) the name and address of the person responsible for the collection of data;
(c)the purpose for which the data is required;
(d) whether or not the supply of the data by the data subject is discretionary or mandatory;
(e) the consequences of failure to provide the data;
(f) the authorised requirement for the collection of the information or the requirement by law for its collection;
(g) the recipients of the data;
(h) the existence of the right of access to and the right to request rectification of the data collected before the collection; and
(i) the period for which the data will be retained to achieve the purpose for which it is collected.

GDPR	The Act

When data is from third party

GDPR	The Act
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.	Section 13(2): Where the data is collected from a third party, the data subject shall be given the information specified in subsection (1) before the collection of the data or as soon as practicable after the collection of the data. (3) Subsection (2), shall not apply- (a) where it is necessary to avoid the compromise of the law enforcement power of a public body responsible for the prevention, detection, investigation, prosecution or punishment of an offence; (b) information relating to national security; (c) to information relating to the enforcement of a law which imposes a pecuniary penalty; (d) to information relating to the enforcement of legislation which concerns public revenue collection; (e) to information relating to the preparation or conduct of proceedings before a court or tribunal.

Intelligibility requirements

GDPR	The Act
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

GDPR	The Act
See Article 12(1) above.	The Act does not explicitly refer to format requirements.

GDPR	The Act

Exceptions

GDPR	The Act
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 where information is collected directly from data subjects. In relation to data collected from third parties Section 13(3) stipulates: Subsection (2), shall not apply- (a) where it is necessary to avoid the compromise of the law enforcement power of a public body responsible for the prevention, detection, investigation, prosecution or punishment of an offence; (b) information relating to national security: (c) to information relating to the enforcement of a law which imposes a pecuniary penalty; (d) to information relating to the enforcement of legislation which concerns public revenue collection; (e) to information relating to the preparation or conduct of proceedings before a court or tribunal.

5.3. Right to object

While both the GDPR and the Act provide for the right to object or to prevent processing, there are significant variations in when and how these rights apply. In particular, the Act limits the right to object to instances where 'unwarranted substantial damage or distress' is or is likely to be caused.

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 7(3): Except for data collected or processed under subsection (2), where a data subject objects to the collection or processing of personal data, the person who is collecting or processing the personal data shall stop the collection or processing of the personal data.

Section 25(1): A data subject shall at any time by notice in writing to a data controller or data processor, require the data controller or data processor to stop processing personal data which causes or is likely to cause unwarranted substantial damage or distress to the data subject.

Section 10(1) of the Regulations: Subject to subregulation (2), a data subject who objects to the collection or processing of his or her personal data, shall notify the data collector, data processor or data controller of the objection.

Section 36(1) of the Regulations: A data subject may require the data controller to cease the processing of personal data where the processing is not compatible with the purpose for which the personal data was collected.

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.

While the Act does not specifically refer to consent withdrawal, Section 7 provides that consent is required unless exceptions apply. See Section 7(3) of the Act above.

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:

The Act does not explicitly refer to a similar requirement to restrict processing.

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.

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.

Section 26(1): A data subject may by notice in writing to a data controller, require the data controller to stop processing his or her personal data for purposes of direct marketing.

(3) Subject to sub-section (1) a data subject may enter into agreement with a data controller for purposes of using or processing his or her personal data for pecuniary benefits.

(2) A data controller shall within fourteen days after receipt of the notice inform the data subject in writing that the data controller has complied or intends to comply with the notice of the data subject, or of the reasons for non-compliance.

(4) Where the data controller gives reasons for non-compliance, a copy of the notice required by subsection (2) shall be given to the PDPO within the time specified in that subsection.

(5) Where the PDPO is satisfied that the notice in subsection (1) is justified, the PDPO may direct the data controller to comply.

(6) In this section 'direct marketing' includes the communication by whatever means of any advertising or marketing material which is directed at an individual.

GDPR	The Act

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.

The Act does not explicitly refer to a requirement to inform data subjects of their right to prevent processing.

Fees

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

Article 16(2): The personal data subject shall have the right to object at any time and free of charge.

Response timeframe

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

Section 25(2): A data controller shall within fourteen days after receipt of a notice inform the data subject in writing that the data controller has complied or intends to comply with the notice of the data subject, or of the reasons for non-compliance.

(3) Where the data controller gives reasons for non-compliance, a copy of the notice required by subsection (2) shall be given to the PDPO within fourteen days.

(4) Where the PDPO is satisfied that the data subject is justified, the PDPO shall direct the data controller to comply within seven days.

Section 36(3) of the Regulations: Where the data controller does not comply with the notice, the data controller shall state the reasons for non-compliance.

(4) Where a data controller gives reasons for non-compliance, a copy of the notice provided by the data subject, shall be given to the PDPO.

(5) Where the PDPO does not agree with the reasons for non-compliance, the PDPO shall direct the data controller or data processor to comply with the notice of the data subject, within seven days.

Section 37(1) of the Regulations: Where a data processor or data controller notifies the data

GDPR	The Act

Response timeframe

subject of his or her intention to continue processing personal data for the purpose of direct marketing, the data subject may within 14 days of receiving the notice request the PDPO in writing to review the decision of the data controller or data processor.

(2) The PDPO shall review the decision of the data controller or data processor within 14 days after receiving the request of the data subject.

Format of response

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

Schedule 1, Form 1, of the Regulations outlines a notice of objection to the collection/processing of personal data.

Exceptions

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

Section 25(5): This Section does not apply to data collected or processed in accordance with section 4(2). [Section 4(2) refers to the establishment of the data protection office]

Under Section 10(2) of the Regulations, the right to object does not apply to personal data provided under Section 7(2) of the Act, and to personal data which is the subject to the legitimate interest of a data collector, processor, or controller.

(3) For the purposes of subregulation (2)(b), 'legitimate interest' is the processing of personal data in a manner that the data subject would reasonably expect or where there is a compelling justification for the processing and includes the processing of data to prevent fraud, maintain network and information security, prevent of crime or threats to public security, internal administrative purposes.

(4) The burden to establish a legitimate interest lies with the data collector, data processor or data controller.

5.4. Right of access

Like the GDPR, the Act establishes a right of access, however the provisions regulating the specific information to be accessed are more detailed in the GDPR. Both pieces of legislation require that data subjects are informed of the right to 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 24(1): A data subject who provides proof of identity may request a data controller to-

(a) confirm whether or not the data controller holds personal data about that data subject;

(b) give a description of the personal data which is held by the data controller;

(c) provide the identity of a third party or a category of a third party who has or has had access to information.

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;

Section 24(1): A data subject who provides proof of identity may request a data controller to-

(a) confirm whether or not the data controller holds personal data about that data subject;

(b) give a description of the personal data which is held by the data controller;

(c) provide the identity of a third party or a category of a third party who has or has had access to information.

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 13(1): (1) A person collecting personal data shall inform the data subject about- [...] (h) the existence of the right of access to and the right to request rectification of the data collected before the collection.

Fees

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

The Act does not explicitly refer to fees or charges in relation to this right.

Verify data subject request

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

Section 13(3): A data controller shall not comply with a request under this section unless the data controller is given information that the data controller may reasonably require to identify the person making the request and to locate the data requested by that person.

Section 35(2) of the Regulations: A data subject satisfies the proof of identity where the data subject provides, a national identification card or alien's identification card, a passport or any travel document, or a driver's license.

GDPR	The Act

Response timeframe

See Article 12(3) in section 5.1. above.	Section 13(9): Subject to subsection (4), a data controller shall comply with a request under this Section promptly and in any event within thirty days from the date of receipt of the request. Section 35(3) of the Regulations provide a data controller must inform data subjects of its decision within seven days of receipt of the request.

Format of response

See Article 12(1) in section 5.1. above.	The Act does not explicitly refer to the format of response beyond the information in Section 24 (see above).

Exceptions

See Article 12(5) in section 5.1. above.	Section 13(4): Where a data controller is unable to comply with the request without disclosing data related to another individual who may be identified from the information, the data controller shall not comply with the request unless- (a) the other individual consents to the disclosure of the data to the person who makes the request; (b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual; or (c) compelled by a court order. (5) For the purposes of subsection (4)- (a) a reference to data related to another individual includes a reference to data which identifies that individual as the source of the data requested; and (b) another individual may be identified from the data disclosed if that individual can be identified from that data, or any other data which in the reasonable belief of the data controller are likely to be in, or come into the possession of the data subject who made the request.

GDPR | The Act

Exceptions (cont'd)

See Article 12(3) in section 5.1. above.	(6) A data controller shall not use subsection (4) as an excuse for failing to communicate so much of the information sought that may be communicated without the disclosure of the identity of the individual concerned. (7) The data controller may make the communication under subsection (6) by omitting or deleting the name or other identifying particulars of the other individual. (8) For the purposes of subsection (4), to determine whether it is reasonable to comply with the request without the consent of the other individual concerned, the data controller shall take into account- (a) any duty of confidentiality owed to the other individual; (b) any steps taken by the data controller to seek the consent of that other individual; (c) whether the other individual is capable of giving consent; and (d) any express refusal of consent by the other individual.

5.5. Right not to be subject to discrimination

Consistent

Neither the GDPR nor the Act explicitly provide a definition for a general right to non-discrimination for the exercise of rights. Both pieces of legislation, however, establish rights for data subjects not to be subject to decisions made solely through automated processing.

GDPR	The Act

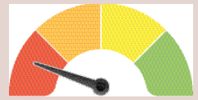
Definition of right

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]	Section 27(1): A data subject may by notice in writing to a data controller require the data controller to ensure that any decision taken by or on behalf of the data controller which significantly affects that data subject is not based solely on the processing by automatic means of personal data in respect of that data subject. [Section 27 of the Act goes on to detail this right, including exceptions whereas Section 38 of the Regulations outlines format and response times]

5.6. Right to data portability



Inconsistent

Unlike the GDPR, the Act does not explicitly refer to a 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.	The Act does not explicitly refer to a right to data portability.

Inform data subject of right

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

Fees

GDPR	The Act
See Article 12(5) in section 5.1. above.	The Act does not explicitly refer to a right to data portability.

Response timeframe

GDPR	The Act
See Article 12(3) in section 5.1. above.	The Act does not explicitly refer to a right to data portability.

Format

GDPR	The Act
See Article 20(1) above.	The Act does not explicitly refer to a right to data portability.

Controller to controller

GDPR	The Act
Article 20(2): In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.	The Act does not explicitly refer to a right to data portability.

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

6. Enforcement

6.1. Monetary penalties

There are several similarities between the GDPR and the Act, including that they both establish the potential for significant monetary penalties equivalent to millions of euros or percentages of global annual turnover. A key difference between the pieces of legislation, however, is that the Act provides for potential prison terms and that individuals may be held liable for offences.

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.	Section 5(1): For purposes of this Act and in addition to its functions under any other law, the personal data protection office shall- (a) oversee the implementation of and be responsible for the enforcement of this Act.
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).	The maximum stated monetary penalty under the Act is equivalent to 245 currency points' (Section 37(2) of the Act), which is UGX 4.9 million (approx. €1,240).

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.

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.

Section 38(1): Where an offence under Sections 31 and 32 is committed by a corporation, the corporation and every officer of the corporation who knowingly and willfully authorises or permits the contravention is liable to the offence.

(2) A court which convicts a person under subsection (1) may, in addition to the punishment order the corporation, pay a fine not exceeding two percent of the corporation's annual gross turnover.

Mitigating factors

Article 83(2): When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

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

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

Section 38(3): A court shall take into consideration the gravity of the offence under subsection (1) and its impact in determining the fine to impose under subsection (2).

GDPR | The Act

Mitigating factors (cont'd)

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(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.

Part VII of the Act established that penalties may include a prison term not exceeding 10 years.

DPO liability

Not applicable.

Section 38(1): Where an offence under Sections 31 and 32 is committed by a corporation, the corporation and every officer of the corporation who knowingly and willfully authorises or permits the contravention is liable to the offence.

6.2. Supervisory authority

Fairly consistent

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

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 4(1): There is established a PDPO responsible for personal data protection under NITA-U which shall report directly to the Board.

Section 5(3): The office in performing its functions under this Act shall not be under the direction or control of any person or Authority.

Section 3(1) of the Regulations provides for the establishment of a PDPO in the NITA-U. (2) The PDPO shall be under the general supervision of the Board of Directors of the NITA-U.

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;

Section 5(1): For purposes of this Act and in addition to its functions under any other law, the PDPO shall-

[...] (c) monitor, investigate and report on the observance of the right to privacy and of personal data;

[...] (e) receive and investigate complaints relating to infringement of the rights of the data subject under this Act;

[...] (2) The office shall have all powers necessary for the performance of its functions under this Act.

Section 4 of the Regulations provide, in addition to those functions specified in Section 5 of the Act, the PDPO shall

[...]

(e) conduct audits to ensure compliance by data collectors, processors, controllers and data subjects with the Act and the Regulations and address potential issues proactively.

GDPR	The Act

Investigatory powers (cont'd)

(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.

Corrective powers

Article 58(2): Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

Section 5(1): For purposes of this Act and in addition to its functions under any other law, the PDPO shall-

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

[...] (e) receive and investigate complaints relating to infringement of the rights of the data subject under this Act;

[...] (g) perform such other functions as may be prescribed by any other law or as the office considers necessary for the promotion, implementation and enforcement of this Act;

(2) The office shall have all powers necessary for the performance of its functions under this Act.

Section 4 of the Regulations provide the PDPO shall:

[...] (b) coordinate, supervise and monitor data collectors, data processors, data controllers and data subjects on all matters relating to the Act; and

[...] (d) set, monitor and regulate standards for personal data protection and privacy.

GDPR	The Act

Corrective powers (cont'd)

(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

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 5(1): For purposes of this Act and in addition to its functions under any other law, the PDPO shall-

[...] (b) promote the protection and observance of the right to the privacy of a person and of personal data;

[...] (d) formulate, implement and oversee programmes intended to raise public awareness about this Act;

[...] (f) establish and maintain a data protection and privacy register;

[...] (2) The office shall have all powers necessary for the performance of its functions under this Act.

Section 4 of the Regulations provide the PDPO shall:

[...] (a) provide guidance to data collectors, processors, data controllers, and data subjects about their data protection and privacy rights, obligations and responsibilities under the Act;

[...] (f) provide guidance to Government on matters of data protection and privacy;

[...] (h) issue recommendations to institutions about the interpretation or application of data protection and privacy rules.

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 5(1): For purposes of this Act and in addition to its functions under any other law, the PDPO shall-

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

(b) promote the protection and observance of the right to the privacy of a person and of personal data;

(c) monitor, investigate and report on the observance of the right to privacy and of personal data;

(d) formulate, implement and oversee programmes intended to raise public awareness about this Act;

(e) receive and investigate complaints relating to infringement of the rights of the data subject under this Act;

(f) establish and maintain a data protection and privacy register;

(g) perform such other functions as may be prescribed by any other law or as the PDPO considers necessary for the promotion, implementation and enforcement of this Act;

(2) The office shall have all powers necessary for the performance of its functions under this Act.

Section 4 of the Regulations: In addition to the functions specified in Section 5 of the Act, the PDPO shall:

- provide guidance to data collectors, data processors, data controllers, and data subjects about their data protection and privacy rights, obligations and responsibilities under the Act;

- coordinate, supervise and monitor data collectors, data processors, data controllers and data subjects on all matters relating to the Act;

- build capacity of management of the PDPO and staff on compliance requirements under the Act and these regulations;

- set, monitor and regulate standards for personal data protection and privacy;

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

- conduct audits to ensure compliance by data collectors, data processors, data controllers and data subjects with the Act and these regulations and address potential issues pro actively;

- provide guidance to Government on matters of data protection and privacy;

- undertake or commission research as may be necessary to promote the objects of the Act; and

- issue recommendations to institutions about the interpretation or application of data protection and privacy rules.

Section 5 of the Regulation: The PDPO may (a) establish a mechanism for collaboration and promotion of partnerships between various categories of players in data protection and privacy; and (b) charge fees for services provided by the PDPO.

Section 6 of the Regulations: The PDPO shall cooperate with other government ministries, departments and agencies in the implementation of the Act and regulations.

Section 13(1) of the Regulations: The PDPO must keep and maintain the data protection and privacy register, provided under Section 29 of the Act, in electronic or manual form.

(2) The PDPO must keep the Register up to date.

Section 42(1) of the Regulations provide, where a complaint is made to the PDPO under Sections 39 and 40 of the Regulations, the PDPO must investigate the complaint within 21 days of receipt of the complaint.

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.

The Act does not explicitly refer to annual reports, although it does establish that the PDPO should report to NITA-U under Section 5.

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 33(1): Where a data subject suffers damage or distress through the contravention by a data controller, data processor or data collector of the requirements of this Act, that data subject is entitled to apply to a Court of competent jurisdiction for compensation from the data collector, data processor or data controller for the damage or distress.

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.

See Section 33(1) of the Act above, which refers to 'damage or 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.

Specifies amount for damages

Not applicable.

The Act does not explicitly refer to an amount for damages.

GDPR	The Act

Processor liability

Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

In general terms, the Act does not differentiate liabilities between data controllers, collectors, or processors. 'Persons' may be held liable for offences under the Act.

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 33(2): In proceedings against a person under this section, it is a defence to prove that the person took reasonable care in all the circumstances to comply with the requirements of this Act.

Section 34 of the Act further establishes a process for appeals against decisions made by the PDPO.