Comparing privacy laws:
GDPR v. POPIA

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

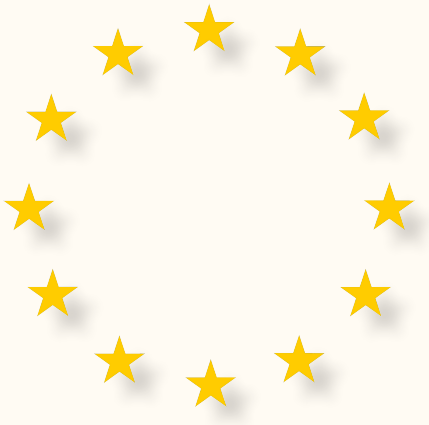
OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

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. South Africa's Protection of Personal Information Act, 2013 (Act 4 of 2013) ('POPIA') was promulgated into law on 26 November 2013, following the President's signature. The Information Regulator ('the Regulator'), the data protection authority provided for by POPIA, held its first meeting late in 2016, although its current operations are still limited. In June 2020, the President announced that certain essential remaining sections of POPIA would commence on 1 July 2020 and that, following a 12-month transition period, public and private bodies would need to be compliant from 30 June 2021. POPIA has also been further supplemented through the Regulations Relating to the Protection of Personal Information (2018) ('the POPIA Regulations'), which set out additional requirements and provide several template forms for a wide range of scenarios.

POPIA and the GDPR contain many similarities, and particularly in regard to their material scope, key definitions, providing for data subject rights, and in their general approaches to personal data protection. However, there are also substantial differences between POPIA and the GDPR, both in broad and detailed terms. For instance, from a wider point of view POPIA does not establish an explicit right to data portability, and it applies to juristic persons. In more nuanced areas, there are variations in what is defined as a special category of data, when data subject rights can be exercised, and how to respond to a data breach.

This report organises provisions from the GDPR and POPIA 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 POPIA.

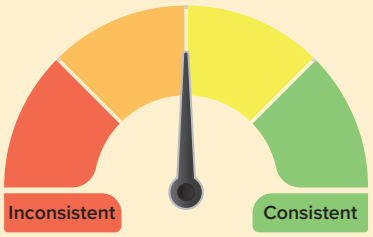
Key for giving the consistency rate

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

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



Usage of the Guide

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

1. Scope

1.1. Personal scope

Fairly consistent

There are general similarities between the GDPR and POPIA in relation to data controllers, responsible parties, processors, operators, and data subjects, as well as the regulation of public bodies. A major difference, however, is that POPIA includes juristic persons under its scope of application. POPIA also does not explicitly refer to matters such as the nationality or place of residence of data subjects, or the treatment of deceased persons' personal data.

GDPR Articles 2, 4(1) Recitals 2, 14, 22-25	POPIA Section 1

Similarities

The GDPR **only** protects **living individuals**. The GDPR does not protect the personal data of deceased individuals, this being left to Member States to regulate.	POPIA **only** protects **living individuals**. POPIA does not protect the personal data of deceased individuals.
The GDPR defines a **data controller** as a 'natural and 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.'	Section 1 of POPIA defines a '**responsible party**' as a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.
The GDPR defines a **data processor** as a 'natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.'	Section 1 of POPIA defines an '**operator**' as a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
The GDPR **applies** to data controllers and data processors who may be public bodies.	POPIA **applies** to responsible parties that may be **public bodies**.

Differences

Article 4(1) of the GDPR clarifies that a **data subject** is 'an identified or identifiable natural person.'	Section 1 of POPIA clarifies that a '**data subject**' means the person to whom personal information relates. In addition, though, POPIA also defines a 'person' as meaning a **natural person or a juristic person**.
The GDPR provides that it 'should apply to natural persons, **whatever their nationality or place of residence**, in relation to the processing of their personal data.'	POPIA **does not explicitly refer** to the nationality or place of residence of data subjects.

1.2. Territorial scope

Fairly inconsistent

Where the GDPR refers to entities being established within the territory of the European Union, POPIA specifies that entities must either be domiciled or use means in South Africa in order to fall under its scope. The GDPR further specifies provisions for the offering of goods and services, and monitoring from abroad, which POPIA does not.

GDPR	POPIA
Articles 3, 4, 11 Recitals 2, 14, 22-25	Section 3

Similarities

The GDPR **applies** to organisations that have presence in the EU. In particular under Article 3, the GDPR applies to entities or organisations established in the EU, notably entities that have an '**establishment**' in the EU or if processing of personal data takes place in the context of the activities of that establishment, irrespective of whether the data processing takes place in the EU or not.

Section 3 of POPIA clarifies that it applies where the responsible party is either **domiciled** in South Africa; or not domiciled in South Africa, but **makes use of automated or non-automated means in South Africa**, unless those means are used only to forward personal information through South Africa.

Differences

In relation to **extraterritorial scope**, the GDPR applies to the processing activities of data controllers and data processors that **do not have any presence in the EU**, where processing activities are related to the **offering of goods, or services to individuals in the EU, or to the monitoring of the behaviour of individuals in the EU**.

POPIA **only** applies where either the responsible party is **domiciled in South Africa or is using means in South Africa**. POPIA does not refer to the offering of goods or services, or monitoring of individuals from abroad.

1.3. Material scope

Fairly consistent

The GDPR, though, also sets out provisions for pseudonymised data. While both the GDPR and POPIA provide for general exemptions, POPIA is more detailed in its regulation of processing for journalistic, literary, and artistic purposes, while the GDPR establishes that these purposes may be further regulated at a Member State level.

GDPR	POPIA
Articles 2-4, 9, 26 Recitals 26	Sections 1, 3, 6, 7, 26-33

Similarities

The GDPR defines '**personal data**' as 'any information' that directly or indirectly relates to an identified or identifiable individual. The GDPR does not apply to the personal data of deceased persons.

Section 1 of POPIA defines '**personal information**' as information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person. In addition, POPIA provides a non-exhaustive list of examples including, for example, another person's opinion of an individual, identifying numbers, or correspondence.

The GDPR applies to the '**processing**' of personal data. The definition of 'processing' covers 'any operation' performed on personal data '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.'

POPIA applies to the '**processing**' of personal information. Section 1 defines 'processing' as 'any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; dissemination by means of transmission, distribution or making available in any other form; or merging, linking, as well as restriction, degradation, erasure or destruction of information.'

The GDPR defines **special categories of personal data** as 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**. The GDPR also provides specific requirements for its processing.

Sections 26-33 of POPIA establish requirements for processing '**special personal information**'. Under Section 26, special personal information is defined as including 'the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject' as well as certain information related to criminal behaviour.

The GDPR **excludes** from its application the processing of personal data by individuals for **purely personal or household purposes**. This is data processing that has 'no connection to a professional or commercial activity.'

Section 6 provides that POPIA **does not apply** to the processing of personal information in the course of a purely personal or household activity.

GDPR	POPIA
Similarities (cont'd)	
The GDPR **excludes** from its application data processing in the context of **law enforcement or national security**.	Section 6 of POPIA also **excludes** from its application processing by or on behalf of a public body for which the purpose is the **prevention or detection of unlawful activities**.
The GDPR provides requirements for specific processing situations including processing for **journalistic purposes and academic, artistic or literary expression**.	Section 7 of POPIA establishes particular exceptions and requirements for processing for **journalistic, literary, or artistic purposes**.
The GDPR applies to the processing of personal data **by automated means or non-automated means if the data is part of a filing system**.	Section 3 of POPIA specifies that it applies to personal information 'entered in a record by or for a responsible party by **making use of automated or non-automated means**. Provided that when the recorded personal information is processed by **non-automated means, it forms part of a filing system** or is intended to form part thereof.'
The GDPR excludes **anonymous data** from its application, which is defined as information that 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 6 excludes personal information that has been **de-identified** to the extent that it cannot be reidentified again.
Differences	
Not applicable.	Not applicable.

2. Key definitions

Consistent

2.1. Personal data

Although the concepts of personal data and personal information are similar in the GDPR and POPIA respectively, POPIA provides a specific list of examples of personal information within its definition while the GDPR describes examples of personal information within its recitals. Definitions of sensitive information, or special categories, as well as consent and biometrics likewise correspond between the two laws.

GDPR	POPIA
Articles 4(1), 9 Recitals 26-30	Sections 1, 6, 26,

Similarities

The GDPR defines '**personal data**' as '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 1 of POPIA defines '**personal information**' as information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- the biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person; and
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

The GDPR defines **special categories of personal data** as data revealing a data subject's 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade

Section 26 of POPIA defines **special personal information** as including 'the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion,

Similarities (cont'd)

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.

health or sex life or biometric information of a data subject' as well as certain information related to criminal behaviour.

The GDPR specifies that **online identifiers** may be considered as personal data, such as **IP addresses, cookie identifiers, and radio frequency identification tags**.

Section 1 of POPIA defines '**unique identifier**' as any identifier that is **assigned to a data subject** and is used by a responsible party for the purposes of the operations of that responsible party and that **uniquely identifies that data subject in relation to that responsible party**.

The GDPR **does not** apply to 'anonymised' data, where the data can no longer be used to identify the data subject.

Section 6 of POPIA excludes personal information that has been **de-identified** to the extent that it cannot be re-identified again.

Differences

Not applicable.

Not applicable.

2.2. Pseudonymisation

Inconsistent

Although POPIA refers to de-identification and re-identification, it does not contain definitions for anonymisation and pseudonymisation. De-identification differs from 'anonymous information', particularly in regard to the concept of 'a reasonably foreseeable method'.

GDPR Articles 4(5), 11 Recitals 26, 29	POPIA Section 1

Similarities

Not applicable.	Not applicable.

Differences

The GDPR defines **pseudonymised data** as 'the processing of personal data in such a manner that the personal data that 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.'

POPIA does **not** refer to 'pseudonymisation.'

'De-identify', in relation to personal information of a data subject, means to delete any information that:

- identifies the data subject;
- can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
- can be linked by a reasonably foreseeable method to other information that identifies the data subject.

2.3. Controllers and processors

Fairly consistent

The concepts of data controllers and processors under the GDPR are comparable with the concepts of responsible parties and operators in POPIA. Furthermore, both the GDPR and POPIA provide that contracts be made between these entities. The GDPR and POPIA differ, however, in relation to Data Protection Impact Assessments ('DPIA') and data protection officer ('DPO') appointments.

GDPR	POPIA
Articles 4, 17, 28, 30, 32, 33, 35, 37, 38 Recitals 64, 90, 93	Sections 1, 20, 21 POPIA Regulations

Similarities

A **data controller** is a natural or legal person, public authority agency or other body that determines the **purposes** and **means** of the processing of personal data, alone or jointly with others.	Section 1 defines a '**responsible party**' as a public or private body or any other person which, alone or in conjunction with others, **determines the purpose of and means** for processing personal information.
A **data processor** is a natural or legal person, public authority, agency or other body which processes personal data on **behalf** of the controller.	Section 1 defines an '**operator**' as a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
The GDPR provides for the designation of a **data protection officer** ('DPO') by data controllers or data processors and defines the role of a DPO (see section 4.4.).	Section 1 of POPIA defines the concept of an '**information officer**', which, for a private body, means the head of a private body as contemplated in Section 1, of the Promotion of Access to Information Act, 2000 (Act 2 of 2000) ('PAIA'). The role of an information officer is further specified in Section 55 (see section 4.4.).
The GDPR requires that processing by a processor is governed by **a contract or other legal act** under Union or Member State law.	Section 21 provides, 'A responsible party must, in terms of a **written contract** between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in Section 19.'
The GDPR provides that where processing is to be carried out on behalf of a controller, the **controller shall use only data processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.	Sections 20 and 21 establish **security measures that are to be undertaken by operators** and further require that responsible parties ensure appropriate measures are implemented by operators through contacts.
In addition, the data processor shall not engage another data processor without prior specific or general written **authorisation** of the controller.	Section 20 provides that an operator or anyone processing on behalf of an operator must only process information with the **knowledge or authorisation** of the responsible party.

GDPR	POPIA

Similarities (cont'd)

The GDPR provides that a data controller or data processors conduct **Data Protection Impact Assessments** ('DPIA') in certain circumstances (see section 4.3.).

POPIA itself does **not** establish equivalent provisions for DPIA. However, Section 4(b) of the POPIA Regulations outline that the responsibilities of information officers include conducting a **personal information impact assessment** to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.

Differences

Data controllers based outside the EU and involved in certain forms of processing, with exceptions based on the scale of processing and type of data, are obliged to **designate a representative based within the EU** in writing.

POPIA does **not** explicitly refer to a requirement to have a representative based within South Africa.

2.4. Children

Inconsistent

POPIA offers a much higher age threshold for children (under 18) compared to the GDPR (between 13 and 16). POPIA also provides general restrictions on processing children's personal information, while the GDPR primarily refers to children's personal data in the context of information society services. Furthermore, POPIA explicitly leaves room for the Information Regulator to establish additional requirements.

GDPR	POPIA
Articles 6, 8, 12, 40, 57 Recitals 38, 58, 75	Sections 1, 34, 35

Similarities

GDPR	POPIA
Not applicable.	Not applicable.

Differences

GDPR	POPIA
The GDPR **does not** define 'child' nor 'children.'	Under Section 1 of POPIA, '**child**' means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him or herself.
Where the processing is based on consent, the consent of a parent or guardian is required for providing information society services to a child below the **age of 16**. EU Member States can **lower this age limit to 13**.	Section 35 of POPIA provides that the personal information of a child may be processed if consent is obtained from a relevant competent person among other exceptions. A child is defined as being under **18 years of age**.
The GDPR considers children as '**vulnerable natural persons**' that merit specific protection with regard to their personal data. In particular, specific protection should be given when children's personal data is used for marketing or collected for information society services offered directly to a child.	POPIA does **not** refer to 'vulnerable' persons. Section 34 establishes **general prohibitions** against processing children's information that apply to all processing, not just marketing or information services.
When any information is addressed specifically to a child, controllers must take **appropriate measures** to provide **information** relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, that the child can easily understand.	Section 35 provides that the Information Regulator may clarify measures and 'impose reasonable conditions' for processing personal information of children. Such conditions have **not** yet been published.
The GPDR provides that data controllers are required to make reasonable efforts to verify that consent is given or authorised by a parent or guardian.	POPIA does **not** specifically refer to verifying the identity of such a competent person.

2.5. Research

Fairly consistent

While POPIA does not offer the same level of detail as the GDPR, it does similarly provide exceptions from certain requirements where processing is for historical, statistical, or research purposes. There are also similar provisions in the GDPR and POPIA in relation to appropriate safeguards and compatibility with original purposes.

GDPR	POPIA
Articles 5(1)(b), 9(2)(j), 14(5), 17(3), 21(6), 89 Recitals 33, 159-161	Sections 14, 15, 18, 32, 35, 37

Similarities

According to the GDPR, **the processing of sensitive data is not prohibited when 'necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.'

Section 27 provides that **special information may be processed when 'processing is for historical, statistical or research purposes** to the extent that the purpose serves a public interest and the processing is necessary for the purpose concerned; or it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent.'

Under the GDPR, the processing of personal data for research purposes is subject to **specific rules** (e.g. with regard to the purpose limitation principle, right to erasure, data minimisation and anonymisation etc.).

POPIA provides **particular requirements** and exceptions where research is the purpose for processing personal information (e.g. record-keeping, appropriate safeguards).

The GDPR provides that '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**'.

Section 15 establishes that 'The further processing of personal information **is not incompatible** with the purpose of collection if [...] the information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form.'

Differences

The GDPR clarifies that 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.'

Although POPIA does **not** explicitly refer to scientific research, nor does it define the general concept of research, it does provide exemptions from several requirements if processing is conducted for 'historical, statistical, or research purposes'.

The data subject has the **right to object** to the processing of personal data for research purposes **unless such research purposes are for reasons of public interest**.

POPIA does **not** explicitly refer to a right to object specifically in relation to research purposes.

GDPR	POPIA

Differences (cont'd)

Under the GDPR, where personal data are processed for research purposes, it is possible for **Member States to derogate from some data subjects' rights**, including the right to access, the right to rectification, the right to object and the right to restrict processing, insofar as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such **derogations** are necessary for the fulfilment of those purposes.

POPIA does **not** have equivalent provisions.

3. Legal basis

Consistent

The GDPR and POPIA provide almost identical legal grounds for the processing of personal data/information. They both also set out specific legal bases for processing sensitive information, define conditions for consent, including the capacity to withdraw consent, and provide exceptions for processing for journalistic and artistic purposes.

GDPR	POPIA
Articles 5-10 Recitals 39-48	Sections 1, 11, 27-33

Similarities

The GDPR states that data controllers can only process personal data when there is a legal ground for it. The legal grounds are:

- **consent**;
- when processing is necessary for the **performance of a contract** which the data subject is part of in order to take steps at the request of the data subject prior to the entering into a contract;
- compliance with **legal obligations** to which the data controller is subject;
- to protect the **vital interest** of the data subject or of another natural person;
- performance carried out in the **public interest** or in the official authority vested in the data controller; or
- for the **legitimate interest** of the data controller when this does not override the fundamental rights of the data subject. Further permissible uses are provided for the processing of special categories of personal data under Article 9(2).

There are specific **legal grounds for processing special categories of data**, such as explicit consent.

The GDPR recognises **consent** as a legal basis to process personal data and includes **specific information** on how consent must be obtained and can be withdrawn.

The GDPR defines 'consent' as '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 11 of POPIA establishes, 'Personal information may only be processed if:

- the data subject or a competent person where the data subject is a child **consents** to the processing;
- processing is necessary to carry out actions for the conclusion or **performance of a contract** to which the data subject is party;
- processing complies with an **obligation imposed by law** on the responsible party;
- processing protects a legitimate **interest of the data subject**;
- processing is necessary for the proper performance of a **public law duty by a public body**; or
- processing is necessary for pursuing the **legitimate interests** of the responsible party.'

There are specific **legal grounds for processing special personal information** in Sections 27-33.

POPIA recognises **consent** as a legal basis to process personal data and includes **specific information** on how consent must be obtained and can be withdrawn.

Section 1 defines 'consent' as '**voluntary, specific and informed expression** of will in terms of which permission is given for the processing of personal information.'

GDPR	POPIA
Differences (cont'd)	
Not applicable.	Not applicable.

4. Controller and processor obligations

4.1. Data transfers

While both the GDPR and POPIA provide restrictions on data transfers, POPIA specifies fewer mechanisms that would enable such transfers and does not detail a process for recognising adequate protection. Both the GDPR and POPIA, however, outline that binding corporate rules ('BCR') may be used to facilitate international data transfers.

GDPR Articles 44-50 Recitals 101, 112	POPIA Section 72

Similarities

The GDPR allows personal data to be transferred to a third country or international organisation that has an **adequate level of protection** as determined by the EU Commission.

Section 72 of POPIA prohibits the international transfer of personal information unless the recipient is subject to a law, binding corporate rules, or binding agreement which provide an **adequate level of protection**.

One of the following **legal grounds** can be applied to the transfer of personal data abroad:

- prior **consent;**
- when a data subject has explicitly **consented** to the proposed transfer and acknowledged the possible risks of such transfer due to inadequate safeguards;
- when the transfer is necessary for the performance or conclusion of a **contract**;
- when the transfer is necessary for important **public interest** reasons;
- when the transfer is necessary for the establishment, exercise, or defence of a **legal** claim; and
- when the transfer is necessary to protect the **vital interests** of a data subject or other persons.

Section 72 also provides the following grounds for data transfers:

- the data subject **consents** to the transfer;
- the transfer is necessary for the **performance of a contract** between the data subject and the responsible party, or for the implementation of **pre-contractual measures** taken in response to the data subject's request;
- the transfer is necessary for the conclusion or **performance of a contract concluded in the interest of the data subject** between the responsible party and a third party; or
- the transfer is for the **benefit of the data subject**, and – (i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; and (ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

In the absence of a decision on adequate level of protection, a transfer is permitted when the **data controller or data processor provides appropriate safeguards** with effective legal remedies that ensure the data subjects' rights as

Section 72 establishes that **binding corporate rules** may be used for international data transfers. POPIA does not, though, refer to standard contractual clauses or codes of conduct in relation to cross-border data flows.

Similarities (cont'd)

prescribed under the GDPR. Appropriate safeguards include:

- **binding corporate rules** with specific requirements (e.g. a legal basis for processing, a retention period, complaint procedures, etc.);
- **standard data protection clauses** adopted by the EU Commission or by a supervisory authority;
- an **approved code of conduct**; or
- an **approved certification mechanism**.

Differences

The GDPR specifies that a cross-border transfer is allowed based on **international agreements** for judicial cooperation.

The grounds for a **cross-border transfer includes the transfer being made from a register** which, according to the Union or a Member States' law, is intended to provide information to the public, and which is open to consultation either by the public in general or by any person who can demonstrate a **legitimate interest**, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

POPIA does **not** specifically refer to international agreements in relation to cross-border data transfers.

POPIA does **not** specifically refer to registers in relation to cross-border data transfers.

4.2. Data processing records

Fairly inconsistent

Although POPIA provides that responsible parties must maintain documentation, it does not stipulate details regarding these records. Instead, such matters are left to the PAIA to regulate. The GDPR provides significantly more detail in this area.

GDPR Article 30 Recital 82	POPIA Section 17

Similarities

Data controllers and data processors have an obligation to **maintain a record** of processing activities under their responsibility.

Section 17 of POPIA stipulates that 'A responsible party must **maintain the documentation of all processing operations** under its responsibility as referred to in Section 14 or 51 of PAIA.'

The GDPR **does not** provide general requirements for registering with a supervisory authority.

POPIA **does not** provide general requirements for registering with a supervisory authority.

Differences

The GDPR **prescribes a list of information that a data controller** must record:

- the name and contact details of the **data controller;**
- the **purposes of the processing**;
- a description of the categories of **personal data**;
- the categories of recipients to whom the personal data will be **disclosed**;
- the **estimated period for erasure** of the categories of data; and
- a general description of the technical and organisational **security measures** that have been adopted.

POPIA **does not** itself prescribe the list of information that a responsible party must record, however such information is **referred to in several sections of PAIA**.

The obligations in relation to data processing records are also imposed on the **representatives of data controllers**.

POPIA **does not** contain equivalent provisions, see PAIA for further information.

The GDPR **prescribes a list of information that a data processor** must record:

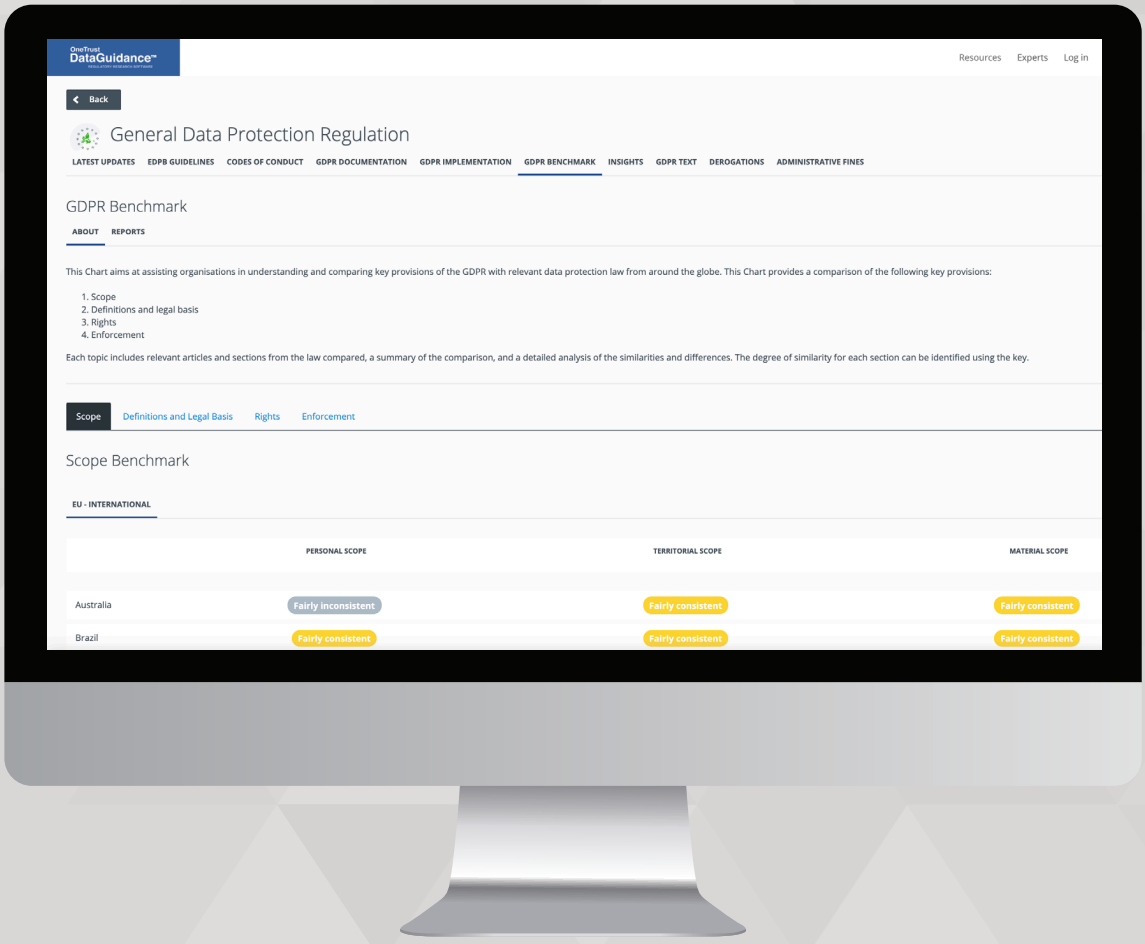
- the name and contact details of the data processor;
- the categories of processing carried out on behalf of each controller;
- international transfers of personal data, with the identification of third countries or international organisations, and the documentation of adopted suitable safeguards; and

POPIA **does not** specify an operator's responsibility to retain documentation. However, responsible parties and operators are required to have a written contract that ensures the operator will establish and maintain certain security measures (see Section 21 of POPIA).

Global Regulatory Research Software

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

Monitor regulatory developments, mitigate risk, and achieve global compliance



OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

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 relivant 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

Start your free trial at
www.dataguidance.com

GDPR	POPIA
Differences (cont'd)	
• a general description of the technical and organisational security measures that have been adopted.	
The processing of information recorded by a data controller shall be in **written or electronic form**.	POPIA **does not** directly address this matter, see PAIA for further information.
The requirements around data processing records shall not apply to **an organisation with less than 250 employees**, unless the processing: • is likely to result in a risk to the rights and freedoms of data subjects; • is not occasional; or • includes special categories of data in Article 9(1) (e.g. religious beliefs, ethnic origin, etc.) or is personal data relating to criminal convictions and offences in Article 10.	POPIA **does not** directly address exceptions, see PAIA for further information.
The GDPR **prescribes a list of information that a data controller** must record **international transfers** of personal data, with the identification of third countries or international organisations, and the documentation of adopted suitable safeguards.	POPIA **does not** specifically address this matter, see PAIA for further information.
The GDPR provides that 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**.	POPIA **does not** contain provisions on this matter, see PAIA for further information.

4.3. Data protection impact assessment

Inconsistent

The GDPR sets out requirements for conducting Data Protection Impact Assessments ('DPIAs'), but POPIA does not.

GDPR Article 35, 36 Recitals 75, 84, 89-93	POPIA POPIA Regulations

Similarities

Under the GDPR, a **DPIA must be conducted** under specific circumstances.	POPIA does not contain equivalent provisions regarding a DPIA. However, Section 4(b) of the POPIA Regulations outline that the **responsibilities of information officers include ensuring a personal information impact assessment** is conducted to make certain that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.

Differences

A data controller is required to, **where necessary**, carry out a review to assess whether the processing of personal data is in accordance with the DPIA, **particularly when there is a change** in risks to processing operations.	POPIA **does not** contain equivalent provisions.
The GDPR provides that a DPIA must be conducted if a data controller utilises **new technologies** to process personal data.	POPIA **does not** contain equivalent provisions.
The GDPR provides that a DPIA must be conducted **under the following circumstances**: • the processing may result in a high risk to the rights and freedoms of an individual; • when a systematic and extensive evaluation of personal aspects relating to natural persons is involved, which is based on automated processing or profiling; • there is processing on a large scale of special categories of data; and • there is systematic monitoring of a publicly accessible area on a large scale.	POPIA **does not** contain equivalent provisions.
The assessment must contain at least the following: • a systematic description of the envisaged processing; • operations and legitimate purposes of the processing;	POPIA **does not** contain equivalent provisions.

GDPR	POPIA

Differences (cont'd)

- the necessity and proportionality of the operations in relation to the purposes; and
- the risks to the rights and freedoms of data subjects.

A data controller **must consult** the supervisory authority prior to any processing that would result in a high risk in the absence of risk mitigation measures as indicated by the DPIA.

POPIA **does not** contain equivalent provisions.

4.4. Data protection officer appointment

Fairly inconsistent

POPIA provides for a similar position as the GDPR's data protection officer ('DPO') in the form of an information officer. The requirements and responsibilities of an information officer, however, are detailed in PAIA and the POPIA Regulations rather than POPIA. In general, the scope of an information officer may be considered to be marignally less expansive than a DPO.

GDPR	POPIA
Articles 13 - 14, 37-39 Recital 97	Sections 1, 55, 56

Similarities

The DPO shall perform a list of tasks including:

- to **inform and advise** the controller or the data processor and the employees who carry out processing of their obligations pursuant to the GDPR and to other Union or Member State data protection provisions;
- to **monitor** compliance with the GDPR with other Union or Member State data protection provisions and with the policies of the data controller or data 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; and
- to **act as a contact point** 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.

Data subjects **may contact** the DPO with regard to the processing of their personal data as well as the exercising of their rights.

Section 55 of POPIA provides sets out an information officer's responsibilities, including:

- the **encouragement of compliance**, by the body, with the conditions for the lawful processing of personal information;
- **dealing with requests** made to the body pursuant to POPIA;
- **working with the Information Regulator in relation to investigations** conducted pursuant to Chapter 6 in relation to the body;
- **otherwise ensuring compliance** by the body with the provisions of POPIA; and
- as may be prescribed.

The POPIA Regulations set out further responsibilities for information officers such as maintaining compliance frameworks, conducting impact assessments, and ensuring awareness sessions are conducted.

One of the tasks of an information officer is to **respond to requests** made to the responsible body pursuant to POPIA.

Differences

Under the GDPR, data controllers and data processors, including their representatives, are required to **appoint** a DPO. The data controller and the data processor shall designate a DPO in any case where:

- the processing is **carried out by a public authority or body**, except for courts acting int heir judicial capacity;
- the core activities of a data controller or data process or consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require **regular and**

Section 1 of POPIA defines the concept of an '**information officer**', which, for a private body, means the head of a private body as contemplated in Section 1, of the PAIA. The role of an information officer is further specified in Section 55 (see section 4.4.).
POPIA also provides for '**deputy information officers**' in Section 56. Each public and private body must make provision, in the manner prescribed in Section 17 of PAIA, with the necessary changes, for the designation of such a

GDPR	POPIA
Differences (cont'd)	
systematic monitoring of data subjects on a large scale; or • the core activities of the controller or the processor relate to a large scale of **special categories of personal data** (e.g. religious beliefs, ethnic origin, data required for the establishment, exercise, or defence of legal claims etc.)	number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in Section 55(1) of POPIA; and any power or duty conferred or imposed on an information officer by POPIA to a deputy information officer of that public or private body.
Contact details of the DPO must be included in the privacy notice for data subjects, and they must be communicated to the supervisory authority.	Officers must take up their duties in terms of POPIA only after the responsible party has **registered them with the Information Regulator**.
A group may appoint a **single DPO** who must be easily contactable by each establishment.	POPIA **does not** contain provisions on this matter, see PAIA for further information.
The DPO shall be designated on the basis of **professional qualities and expert knowledge** of data protection law and practices.	POPIA **does not** contain provisions on this matter, see PAIA for further information.
The GDPR recognises the **independence** of DPOs.	POPIA **does not** contain provisions on this matter, see PAIA for further information.
The DPO must be **provided with the resources necessary** to carry out his or her obligations under the GDPR.	POPIA **does not** contain provisions on this matter, see PAIA for further information.

4.5. Data security and data breaches

Fairly inconsistent

Both the GDPR and POPIA set out significant security requirements and stipulate that data breach notifications be submitted to regulatory authorities and data subjects. However, unlike the GDPR, POPIA provides few exceptions to these notification requirements. Furthermore, POPIA enables the Information Regulator to direct responsible parties to make public data breach notifications.

GDPR	POPIA
Article 5, 24, 32-34 Recitals 74-77, 83-88	Sections 19, 20, 21

Similarities

The GDPR recognises **integrity** and **confidentiality as fundamental principles** of protection by stating that personal data must be processed in a manner that ensures appropriate security of the personal data. The GDPR states that **data controllers and data processors are required to implement appropriate technical and organisational security measures** to ensure that the processing of personal data complies with the obligations of the GDPR.

Section 19 explicitly specifies that 'A responsible party **must secure the integrity and confidentiality** of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures.'

In the case of a personal data breach, the **data controller must notify the competent supervisory authority** of the breach, unless the personal data breach is unlikely to **result in a risk** to the individuals' rights and freedoms.

Section 22 provides that where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party **must notify the Information Regulator**.

The GDPR states that **data processors must notify** the data controller without **undue delay** after becoming aware of the personal data breach.

Section 21 provides, '**The operator must notify the responsible party immediately** where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.'

The GDPR provides a **list** of **technical and organisational measures**, where appropriate, that data controllers and data processors must implement such as pseudonymisation, encryption and the ability to restore availability and access to personal data in a timely manner in the event of physical or technical incidents, to ensure integrity and confidentiality.

Section 19 sets out the following '**reasonable measures**' that should be taken:

- identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- establish and maintain appropriate safeguards against the risks identified;
- regularly verify that the safeguards are effectively implemented; and
- ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

GDPR	POPIA

Similarities (cont'd)

	The responsible party should also have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.
The GDPR provides a **list of information** that must be, at minimum, included in the notification of a personal data breach. For example, a notification must describe the nature of the breach, the approximate number of data subjects concerned, and the consequences of the breach.	Section 22 of POPIA specifies information that should be included in a data breach notification to a data subject, and emphasises that the responsible party 'must provide **sufficient information to allow the data subject to take protective measures** against the potential consequences of the compromise'. Such information includes, where applicable: • a description of the possible consequences; • a description of the measures that the responsible party intends to take or has taken; • a recommendation with regard to the measures to be taken by the data subject; and • if known to the responsible party, the identity of the unauthorised person who may have accessed the personal information.

Differences

Under the GDPR, a personal data breach must be notified to the supervisory authority **without undue delay** and, where feasible, **no later than 72 hours** after having become aware of the breach.	Section 22 outlines that the notification referred must be made **as soon as reasonably possible** after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.
The controller must **notify** the **data subject** of a data breach without undue delay if the data breach is likely to result in a high risk to the rights and freedoms of natural persons.	Under Section 22, the responsible party must also **notify affected data subjects as soon as reasonably possible**.
Under the GDPR, the obligation of data controllers to notify data subjects when the data breach is likely to result in a high risk to the rights and freedoms of natural persons, is **exempted in certain circumstances** such as where: • appropriate technical and organisational protective measures have been implemented; • any subsequent measures have been taken in order to ensure that the risks are no longer likely to materialise; or • it would involve is proportionate effort.	The only exception to the requirement to notify data subject under Section 22 is where the **identity of the data subject cannot be established**. The notification can be delayed if such notification may impede a criminal investigation.

4.6. Accountability

Consistent

Both the GDPR and POPIA specify accountability as a central principle, however POPIA does not explicitly refer to different liabilities between responsible parties and operators.

GDPR	POPIA
Articles 5, 24-25, 35, 37 Recital 39	Sections 8

Similarities

GDPR	POPIA
The GDPR recognises **accountability** as a fundamental principle of data protection. Article 5 states that 'the data controller shall be responsible and able to demonstrate compliance with, paragraph 1 [accountability].' In addition, the principles can be taken to apply to several other principles as mentioned in other sections of this report, including the appointment of a DPO, and DPIAs.	POPIA recognises **accountability** as a fundamental condition or principle. Section 8 states, 'The responsible party must ensure that the conditions set out in this Chapter, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.'

Differences

GDPR	POPIA
Not applicable.	Not applicable.

5. Rights

5.1. Right to erasure

Fairly inconsistent

Both the GDPR and POPIA provide that data subjects may request the deletion or erasure of their data in certain circumstances, however the scope of this right is more limited in POPIA. POPIA is also less explicit in detailing requirements for fees, timeframes for responses, and informing data subjects of their rights, and does not refer to publicly available personal information in the context of the right to deletion. The POPIA Regulations, however, include a template form for data subject deletion requests.

GDPR	POPIA
Articles 12, 17 Recitals 59, 65-66	Sections 18, 23, 24

Similarities

The right to erasure applies to specific grounds, such as where **consent of the data subject is withdrawn** and there is **no other legal ground** for processing, or the personal data **is no longer necessary** for the purpose of which it was collected.

Under Section 24 of POPIA, a data subject may request a responsible party to, '**correct or delete personal information** about the data subject in its possession or under its **control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or destroy or delete a record** of personal information about the data subject **that the responsible party is no longer authorised to retain** in terms of Section 14.'

The right can be exercised **free of charge**. There may be some instances, however, where a fee may be requested, notably when requests are unfounded, excessive, or have a repetitive character.

POPIA **only** directly refers to fees for the exercise of rights in relation to the right to access (see section 5.4. below).

Data subjects **must be informed** that they have the right to request for their data to be deleted and are entitled to ask for their data to be erased.

Section 18 provides that a data subject **should be informed** of the right to access and the **right to rectification**. The right to rectify includes the potential requesting deletion of information under Section 24 of POPIA.

Differences

Exceptions to the right of erasure provided by the GDPR include:

- **freedom of expression** and freedom of information;
- complying with **public interest purposes in the area of public health**;
- establishment, exercise, or defence of **legal claims**; and
- **complying with legal obligations** for a public interest purpose.

POPIA **does not** provide specific exceptions to the right to correction and deletion.

GDPR	POPIA

Differences (cont'd)

Data subject requests under this right must be replied to without 'undue delay and in any event within **one month** from the receipt of request.' The deadline can be extended by **two additional months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such extension within one month from the receipt of the request.	Section 24 establishes that on receipt of a request 'a responsible party must, **as soon as reasonably practicable: correct the information**; • destroy or delete the information; • provide the data subject, to his or her satisfaction, with credible evidence in support of the information; or • where agreement cannot be reached between the responsible party and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.'
A data controller must have in place mechanisms to ensure that **the request is made by the data subject** whose personal data is to be deleted.	In relation to access requests, Section 23 provides that data subject must provide **adequate proof of their identity**.
A request can be made in **writing, orally, and through other means including electronic means** where appropriate.	Section 24 provides that requests must be made in a **prescribed manner**, and Form 2 of the POPIA Regulations consists of the form to be used for requests for correction or deletion or personal information or destroying or deletion of record of personal information in terms of Section 24(1) of POPIA.
If the data controller has made personal data public and is obliged to erase the personal data, the data controller, taking into account the available technology and the cost of implementation, shall take reasonable steps, including **technical measures**, to **inform controllers** processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, such personal data.	POPIA **does not** explicitly refer to the right to correction and deletion in relation to publicly available personal information.

5.2. Right to be informed

Fairly consistent

The GDPR and POPIA both provide for the right to be informed. However, the two laws differ in regard to the specific information that should be notified to data subjects and exceptions to the right to be informed. Furthermore, POPIA is less detailed in terms of format and intelligibility requirements.

GDPR	POPIA
Articles 5-14, 47 Recitals 58-63	Section 18

Similarities

Data subjects have the right to receive information on the following, among other things, at the time of collection where data is collected from them:

- the **identity and the contact details of the controller** or controller's representative;
- the **contact details of the DPO**;
- the **purposes of the processing** as well as the **legal basis for the processing**;
- any **legitimate interests** pursued by the controller or by a third party, if applicable;
- the **recipients or categories of recipients** of the personal data, if any;
- where applicable, the fact that the controller intends to **transfer personal data to a third country** and related information;
- the **period for which the personal data will be stored**, or if that is not possible, the criteria used to determine that period;
- the **data subject's rights**; and
- whether the provision of personal data is an **obligation**.

Section 18 provides that a data subjects receive information on the following, among other things:

- the **information being collected or the source from which it is collected**;
- the **name and address of the responsible party**;
- the purpose of processing;
- whether or not the supply of the information by that data subject is **voluntary or mandatory**;
- the **consequences of failure** to provide the information;
- any **law authorising or requiring the collection**;
- the fact that, where applicable, the responsible party intends to **transfer the information to a third country** or international organisation and related information;
- **recipient or category of recipients** of the information; and
- **data subject rights**.

In addition, data subjects must be informed of the **possible consequences** of a failure to provide personal data whether in complying with statutory or contractual requirements, or a requirement necessary to enter into a contract.

Section 18 establishes that data subjects must be informed of the **possible consequences** of a failure to provide personal information.

A data controller cannot collect and process personal data for purposes other than the ones about which the data subjects were informed, **unless the data controller provides them with further information**.

Under Section 18, data subjects should be **informed of the level of protection** afforded where personal information is to be transferred to a third country or international organisation.

In the case of indirect collection, a data controller must provide information relating to such collection to data

Where information is collected indirectly, Section 18 clarifies that the data subject should be informed

GDPR	POPIA
Similarities (cont'd)	
subjects within a reasonable period after obtaining the data, but at the latest within one month, or **at the time of the first communication with the data subject, or when personal data is first disclosed to the recipient**.	'**before** the information is collected or **as soon as reasonably practicable** after it has been collected.'
Differences	
Information relating to personal data processing (e.g. the purpose of the processing, the rights of data subjects, etc.) must be provided to data subjects by the data controller **at the time when personal data is obtained**.	Section 18 stipulates that information should be provided **prior to collection** where information is collected directly.
The GDPR provides specific information that must be given to data subjects when their personal data has been **collected from a third party**, which includes the sources from which the data was collected.	The information that should be provided **remains the same** regardless of whether data is collected directly or from a third party.
Information should be provided to data subjects in an easily accessible form with clear and plain language, which can be in **writing and other means such as an electronic format**.	POPIA **does not** explicitly refer to intelligibility requirements in relation to the right to be informed.
Data subjects must be informed of the existence of **automated decision-making, including profiling**, at the time when personal data is obtained.	POPIA **does not** contain an equivalent provision.
Information can be provided to data subjects **orally**, in addition to in writing form or electronic means.	POPIA **does not** explicitly refer to format requirements in relation to the right to be informed.
The GDPR **provides examples** of circumstances, which can be considered as 'legitimate interest.'	POPIA **does not** provide examples of legitimate interests.

Fairly consistent

5.3. Right to object

The GDPR and POPIA provide that data subjects may object to processing on certain, limited grounds; however, the laws are not entirely aligned on what these grounds are. While both laws specify that data subjects may object to processing for the purposes of direct marketing, POPIA sets out more requirements on this matter than the GDPR. POPIA, though, is less explicit in relation to fees, response timeframes, and exceptions. The POPIA Regulations, however, include a template form for data subject objection requests.

GDPR Articles 7, 12, 18, 21	POPIA Sections 11, 18

Similarities

Data subjects shall have the right to **withdraw** their consent to the processing of their personal data **at any time**.

Under Section 11, 'The data subject or competent person may **withdraw his, her or its consent [...] at any time**. Provided that the lawfulness of the processing of personal information before such withdrawal or the processing of personal information in terms of subsection (1)(b) to (f) will not be affected.'

Under the GDPR, data subjects are provided with the right to object to the processing of their personal data in specific circumstances:

- the processing of personal data is due to **tasks carried out in the public interest or based on a legitimate interest pursued by the data controller or third party**;
- the processing of personal data is for **direct marketing purposes**; and
- the processing of personal data is for **scientific, historical research or statistical purposes**.

Section 11 establishes that data subjects have the right to object to processing that is carried out for the following purposes:

- protecting **legitimate interests of the data subject**;
- proper performance of **public duty by a public body**;
- **legitimate interests of the responsible or a third party**; and
- **direct marketing**.

The data subject has the right to be **informed** about the right to object.

The data subject has the right to be **informed** about the right to object, as provided for under Section 18.

The GDPR establishes a **right to restrict processing** where:

- the accuracy of the personal data is contested by the data subject;
- the processing is unlawful and the data subject opposes the erasure of the personal data;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject;
- pending the verification of whether the legitimate grounds of the controller override those of the data subject.

POPIA establishes a specific **right to restrict processing** where:

- accuracy of personal information is contested by the data subject;
- the responsible party no longer needs the personal information, but it has to be maintained for purposes of proof;
- the processing is unlawful and the data subject opposes its destruction; or
- the data subject requests to transmit the personal data into another automated processing system.

GDPR	POPIA

Similarities (cont'd)

GDPR	POPIA
Data subjects must be provided with information about **how to exercise** the right.	POPIA **does not** explicitly refer to informing data subjects of how to exercise this right. However, Section 2(1) of the POPIA Regulations outlines that a data subject who wishes to object to the processing of personal information in terms of Section 11(3) of POPIA, must submit Form 1 of the POPIA Regulations to the responsible party.

Differences

GDPR	POPIA
Upon the receipt of an objection request, a data controller shall no longer process the personal data unless: • **the processing is based on a legitimate ground** that overrides the data subjects' interests; or • **it is for the establishment, exercise, or defence of a legal claim**.	POPIA **does not** contain equivalent provisions.

5.4. Right of access

Fairly consistent

The GDPR and POPIA establish similar data subject rights of access to personal data/information. There are, however, differences in relation to potential fees, response timeframes and formats, and exceptions.

GDPR	POPIA
Articles 15 Recitals 59-64	Section 23

Similarities

The GDPR recognises that data subjects have the **right to access** their personal data that is processed by a data controller.

POPIA recognises that data subjects have the **right to access** their personal data that is processed by a data controller.

Differences

The GDPR specifies that, **when responding to an access request**, the data controller must indicate the following information:

- the **purposes** of the processing;
- the **categories** of personal data concerned;
- the recipients or categories of recipients to whom the personal data has been or will be **disclosed**, in particular recipients in third countries or international organisations;
- where possible, the envisaged **period** for which the personal data will be **stored**, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller **rectification or erasure** of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a **complaint** with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their **source**; and
- the existence of **automated decision-making**, including profiling.

Under Section 23, a data subject may request **confirmation** of whether or not the responsible party holds personal information about the data subject; and a **record or a description** of the personal information about the data subject held by the responsible party, including information about the **identity of all third parties, or categories of third parties**, who have, or have had, access to the information.

A data controller can refuse to act on a request when it is **manifestly unfounded, excessive, or has a repetitive character**.

POPIA **does not** directly define to exceptions to the right of access, and instead refers to provisions within PAIA.

The GDPR provides that the right of access must not adversely affect the rights or freedoms of others, **including those related to trade secrets**.

POPIA **does not** directly define to exceptions to the right of access, and instead refers to provisions within PAIA.

GDPR	POPIA
Differences (cont'd)	
The GDPR provides that the right of access **must not adversely affect the rights or freedoms of others**.	POPIA **does not** directly define to exceptions to the right of access, and instead refers to provisions within PAIA.
Data subjects' requests under this right must be replied to without 'undue delay and in any event within **one month** from the receipt of a request.' The deadline can be extended by **two additional months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such an extension within one month from the receipt of a request.	Requests must be responded to '**within a reasonable time**'.
The right to access can be exercised **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive, or have a repetitive character.	The right to confirm that a responsible party holds information must be provided free of charge. A **prescribed fee** may be charged for providing further information. Where a fee is charged, the responsible party must give the applicant a written estimate of the fee before providing the services and may require the applicant to pay a deposit for all or part of the fee.
Data subjects must have a variety of means through which they can make their request, including **orally and through electronic means**. In addition, when a request is made through electronic means, a data controller should submit a response through the same means.	POPIA **does not** explicitly refer to the means through which access requests may be made.
The GDPR specifies that a data controller must **have in place mechanisms** to identify that a request is made by a data subject whose personal data is to be deleted.	Section 23 stipulates that the right to access applies where data subjects **have provided adequate proof of identity**.

5.5. Right not to be subject to discrimination

Consistent

Neither the GDPR nor POPIA specifically defines this right, however it can be considered to be implied in general concepts such as fairness, data subject participation, and lawful processing. The laws similarly protect data subjects from automated decision making.

GDPR	POPIA
Not applicable	Not applicable

Similarities

GDPR	POPIA
The GDPR **does not** explicitly address the right not to be subject to discrimination; therefore, no scope of implementation is defined.	POPIA **does not** explicitly address the right not to be subject to discrimination; therefore, no scope of implementation is defined.

Differences

GDPR	POPIA
Not applicable.	Not applicable.

5.6. Right to data portability

Unlike the GDPR, POPIA does not refer to a right to data portability.

GDPR	POPIA
Articles 12, 20, 28 Recitals 68, 73	Not applicable

Similarities

Not applicable.	Not applicable.

Differences

The GDPR provides individuals with the **right to data portability**.	POPIA **does not** refer to a right to data portability.
The GDPR defines the right to data portability as the **right to receive data processed on the basis of contract or consent and processed by automated means, in a 'structured, commonly used, and machine-readable format'** and to transmit that data to another controller without hindrance.	POPIA **does not** refer to a right to data portability.
The GDPR **does not** explicitly limit the scope of the right to data portability to special categories of personal data.	POPIA **does not** refer to a right to data portability.

6. Enforcement

Fairly inconsistent

6.1. Monetary penalties

The GDPR provides for substantially larger penalties for organisations, including stipulating that monetary penalties may be assessed in the form of a percentage of worldwide turnover. POPIA may support lower financial penalties, but it also sets out provisions for prison sentences and sanctions for individuals.

GDPR Article 83, 84 Recitals 148-149	POPIA Chapter 11

Similarities

The GDPR provides for the possibility of administrative, **monetary penalties** to be issued by the supervisory authorities in cases of non-compliance.

POPIA provides for the possibility of administrative, **monetary penalties** to be issued by the Information Regulator in cases of non-compliance.

When applying an administrative sanction, the supervisory authority must consider:

- the nature, gravity and duration of the infringement;
- the intentional or negligent character of the infringement;
- any action taken to mitigate the damage;
- the degree of responsibility of the controller or processor;
- any relevant previous infringements;
- the degree of cooperation with the supervisory authority;
- the categories of personal data affected by the infringement;
- the manner in which the infringement became known to the supervisory authority;
- 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;
- adherence to approved codes of conduct or approved certification mechanisms; and
- any other aggravating or mitigating factor applicable to the circumstances of the case.

Under Section 109, the **Information Regulator must consider the following factors when determining an appropriate fine**:

- the nature of the personal information involved;
- the duration and extent of the contravention;
- the number of data subjects affected or potentially affected by the contravention;
- whether or not the contravention raises an issue of public importance;
- the likelihood of substantial damage or distress, including injury to feelings or anxiety suffered by data subjects;
- whether the responsible party or a third party could have prevented the contravention from occurring;
- any failure to carry out a risk assessment or a failure to operate good policies, procedures and practices to protect personal information; and
- whether the responsible party has previously committed an offence in terms of POPIA.

Differences

Fines may be **issued directly** by supervisory authorities.

Fines may be **issued directly** by the Information Regulator.

Depending on the violation occurred the penalty may be up to either: **2% of global annual turnover or €10**

Section 109 sets a **fine maximum** of ZAR 10 million (approx. €490,000).

GDPR	POPIA

Differences (cont'd)

million, whichever is higher; or **4% of global annual turnover or €20 million**, whichever is higher.	
The GDPR **does not** establish provisions for imprisonment.	Section 107 sets out **provisions for imprisonment**, which may last up to 10 years for certain violations.
The GDPR **does not** establish DPO or individual liabilities.	POPIA provides for sanctions for persons, which may include **natural or juristic persons**, in Chapter 11.

6.2. Supervisory authority

Fairly consistent

The role of the Information Regulator under POPIA is broadly similar to that of data protection authorities as envisioned by the GDPR. Both have advisory, investigatory, and corrective powers, although the details of these powers differ.

GDPR Articles 51-84 Recitals 117-140	POPIA Chapters 5, 6, 7, 10, 11

Similarities

Under the GDPR, supervisory authorities have **investigatory powers** which include: (i) ordering a controller and processor to provide information required; (ii) conducting data protection audits; (iii) carrying out a review of certifications issued; and (iv) obtaining access to all personal data and to any premises.	Section 40 sets out the powers of the Information Regulator, including **investigatory powers** such as the authority to conduct an assessment, on its own initiative or when requested to do so, of a public or private body, in respect of the processing of personal information by that body for the purpose of ascertaining whether or not the information is processed according to the conditions for the lawful processing of personal information. Sections 89-94 further define the processes for assessments.
Under the GDPR, supervisory authorities have **corrective powers** which include: (i) issuing warnings and reprimands; (ii) imposing a temporary or definitive limitation including a ban on processing; (iii) ordering the rectification or erasure of personal; and (iv) imposing administrative fines.	The Information Regulator has various **corrective powers** which include issuing enforcement notices (see Sections 95-98).
Under the GDPR, supervisory authorities shall also handle **complaints** lodged by data subjects.	Under POPIA, the Information Regulator also handles **complaints** lodged by data subjects.
Under the GDPR, supervisory authorities are tasked with **promoting public awareness** and understanding of the risks, rules, safeguards and rights in relation to processing as well as **promoting the awareness of controllers and processors** of their obligations, amongst other tasks.	The Information Regulator has several **advisory powers**, including issuing codes of conduct and promoting awareness.
Supervisory authorities may be subject to financial control only if it does not affect its **independence**. They have separate, public annual budgets, which may be part of the overall national budget.	Section 39 establishes the **independence** of the Information Regulator.

Differences

It is **left to each Member State to establish a supervisory authority**, and to determine the qualifications required to be a member, and the obligations related to the work, such as duration of term as well as conditions for reappointment.	POPIA **establishes** the Information Regulator under Section 39.

6.3. Other remedies

Fairly consistent

While both the GDPR and POPIA enable data subjects to seek civil remedies for material, or patrimonial, and non-material, or non-patrimonial, damages, there are differences in processes.

GDPR Articles 79, 80, 82 Recitals 131, 146-147, 149	POPIA

Similarities

The GDPR provides individuals with a cause of action to **seek compensation** from a data controller and data processor for a violation of the GDPR.

Section 99 provides that 'A data subject or, at the request of the data subject, the Regulator, **may institute a civil action for damages** in a court having jurisdiction against a responsible party'.

Under the GDPR, the data subject has the right to **lodge a complaint** with the supervisory authority. The supervisory authority must inform the data subject of the progress and outcome of his or her complaint.

Under Section 74 of POPIA, the data subject has the right to **lodge a complaint** with the Information Regulator. The Information Regulator must inform the data subject of the progress and outcome of his or her complaint.

The GDPR provides that a data controller or processor shall be **exempt from liability to provide compensation** if it proves that it is not in any way responsible for the event giving rise to the damage.

Section 99 provides for various **exemptions** from liabilities, including *vis major.*

Differences

The GDPR allows Member States to provide for the possibility for data subjects to give a mandate for representation to a **not-for-profit body, association, or organisation** that has as its statutory objective the protection of data subject rights.

Section 99 establishes the data subject's right to request the Information Regulator to institute a civil action. POPIA **does not** otherwise address this concern.