

BENCHMARKING REPORT

GDPR vs. PDPL



About the authors

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

OneTrust DataGuidance™ Regulatory Research includes focused guidance around core topics (i.e., the GDPR, data transfers, breach notification, among others), comparisons which allow you to compare regulations across multiple jurisdictions at a glance, a daily customized 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 program.

Clyde & Co LLP

With over 5,000 people operating from over 60 offices and associated offices across six continents, Clyde & Co is committed to creating successful outcomes for our clients. Our globally integrated teams of disputes, regulatory, and transactional lawyers provide a comprehensive range of legal services and advice to businesses operating at the heart of global trade and commerce.

Our success in the past 90 years has been built on our vision of a single global partnership, providing a platform that offers rapid access to expertise, wherever you operate in the world.

We're one firm with four core values. We believe that these values reflect our firm, our strategy, and our commitment to delivering commercially-minded legal advice, client-focused services, and innovative technological solutions to support our clients.

Aligned with these values is Clyde & Co's commitment to being a responsible business. We take responsibility for the impact we have on the environment, seeking to reduce it as much and as quickly as possible. We strive to be a positive contributor to the communities in which we operate across our entire global network. We take steps to foster a truly diverse and inclusive workplace, that allows all of our people to flourish, for the benefit of our colleagues, the firm, and our clients.

Contributors:

OneTrust DataGuidance™ Research

Clyde & Co LLP: Jenika Pankhania, Lamiisse Bajunaid, Lama Abumansour, Gianluca de Feo, Masha Ooijevaar, Shamma Sied

Legal Disclaimer

Reproduction of this document without the prior written consent of the copyright owner is prohibited. OneTrust shall have no liability in respect of the use of this document and its contents. This document, its contents, and any information conveyed in relation to it are OneTrust Confidential Information and do not constitute legal advice. Copyright © 2025 OneTrust LLC. Proprietary & Confidential

كليرداندو
CLYDE & CO

Table of content

INTRODUCTION	4
STRUCTURE AND OVERVIEW	5
CONSISTENCY RATING LEGEND	5
1. SCOPE.....	6
1.1. Personal scope	6
1.2. Territorial scope	8
1.3. Material scope	10
2. KEY DEFINITIONS	13
2.1. Personal data	13
2.2. Pseudonymization	15
2.3. Controllers and processors	17
2.4. Children	20
2.5. Research	22
3. LEGAL BASIS.....	24
4. CONTROLLER AND PROCESSOR OBLIGATIONS.....	27
4.1. Data transfers	27
4.2. Data processing records	30
4.3. Data Protection Impact Assessment	32
4.4. Data protection officer appointment	35
4.5. Data security and data breaches	38
4.6. Accountability	41
5. INDIVIDUALS' RIGHTS	42
5.1. Right to erasure	42
5.2. Right to be informed	45
5.3. Right to object	48
5.4. Right to access	50
5.5. Right not to be subject to discrimination in the exercise of rights	54
5.6. Right to data portability	55
6. ENFORCEMENT	57
6.1. Monetary penalties	57
6.2. Supervisory authority	59
6.3. Civil remedies for individuals, including other remedies	62

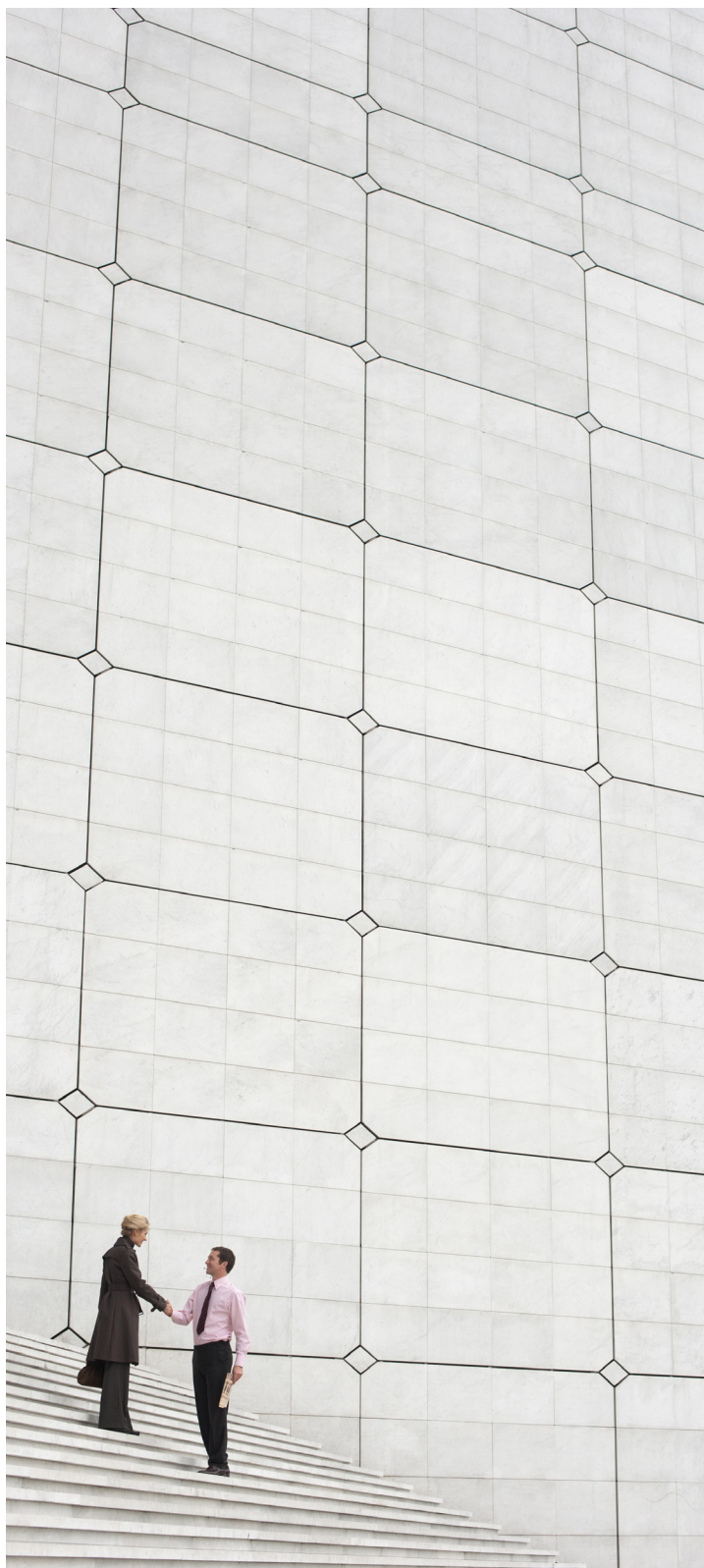
Introduction

The General Data Protection Regulation (GDPR) entered into effect on May 25, 2018, and governs the protection of personal data in EU Member States. Saudi Arabia's data protection law, the Personal Data Protection Law (as amended) (the PDPL, as amended), on the other hand, took effect on September 14, 2023. The Implementing Regulations of the PDPL (the Implementing Regulations) were published on September 7, 2023. The Implementing Regulations expand on the general principles and obligations provided in the PDPL, as amended, and introduce new compliance requirements.

The PDPL, as amended, has many similarities with the GDPR and often uses the same general concepts as well as similar language, particularly with regards to terms such as personal data, pseudonymization, data controller, and processor. In addition, both pieces of legislation apply to the processing of natural persons' data as carried out by controllers and processors and provide special protection for the processing of sensitive personal data. While some foundational elements such as personal and material scope of the laws largely mirror one another, there are key differences between the two pieces of legislation.

The laws adopt very different approaches to the legal bases for processing personal data, with the PDPL, as amended, emphasizing consent as the main legal basis for lawful processing. Notably, the PDPL, as amended, also provides a broader scope of application in relation to, among other obligations, its territorial scope of application, records of processing activities (ROPA), as well as Data Protection Impact Assessments (DPIA). Furthermore, the PDPL, as amended, imposes stricter requirements for the cross-border transfer of personal data. Both laws provide for similar data subject rights, although the GDPR often provides more detailed information surrounding the same.

This Guide is aimed at highlighting the similarities and differences between the two pieces of legislation in order to help organizations develop their compliance activities.



Structure and overview

This Guide provides a comparison of the two pieces of legislation on the following key provisions:

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

Consistency rating legend

			
			
CONSISTENT			
The GDPR and PDPL, as amended, bear a high degree of similarity in the rationale, core, scope, and application of the provision considered.			
			
FAIRLY CONSISTENT			
The GDPR and PDPL, as amended, bear a high degree of similarity in the rationale, core, and scope of the provision considered; however, the details governing its application differ.			
			
FAIRLY INCONSISTENT			
The GDPR and PDPL, as amended, bear several differences with regard to the scope and application of the provision considered; however, its rationale and core present some similarities.			
			
INCONSISTENT			
The GDPR and PDPL, as amended, bear a high degree of difference with regard to the rationale, core, scope, and application of the provision considered.			

1.1. Personal scope



FAIRLY CONSISTENT

The GDPR and the PDPL, as amended, have a similar personal scope of application, applying to public and private entities that process personal data.

However, the personal scope of the PDPL, as amended, is broader than the personal scope of the GDPR, especially considering that the former covers personal data of deceased individuals.

Similarities

GDPR

Articles 3, 4(1), 4(7), and 4(8)
Recitals 2, 14, 22-25, and 27

1. The GDPR applies to public and private entities that process personal data.
2. 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.'
3. 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.'
4. The GDPR protects the personal data of natural persons (i.e., individuals) within the EU, not legal entities.
5. The GDPR clarifies that a data subject is 'an identified or identifiable natural person.'
6. The GDPR applies to data controllers and data processors who may be public bodies.

PDPL, as amended

Articles 1(16), 1(18), 1(19), and 2 of the PDPL, as amended

1. The PDPL, as amended, applies to public and private entities that process personal data.
2. The PDPL, as amended, defines a data controller as any public entity or natural or legal person that specifies the purpose and method of processing personal data, whether such processing is performed by it or by the processor.
3. The PDPL, as amended, defines a data processor as any public entity or any natural or legal person that processes personal data for the benefit and on behalf of a controller.
4. The PDPL, as amended, protects the personal data of natural persons (i.e., individuals) within the Kingdom of Saudi Arabia (KSA), not legal entities.
5. The PDPL, as amended, defines a data subject as the individual to whom the personal data relates.
6. The PDPL, as amended, applies to data controllers and data processors who may be public bodies.

Differences

1. The GDPR covers both data controllers and data processors that handle personal data.
2. 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.
3. The GDPR applies to both data controllers and processors within the EU, as well as those outside the EU if they process personal data of individuals in the EU by offering goods or services or monitoring behavior.
4. 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.'

1. The PDPL, as amended, covers controllers that handle personal data. Nevertheless, the PDPL, as amended, provides detailed requirements for vendor management.
2. The PDPL, as amended, includes the processing of personal data of deceased persons if the personal data leads to the identification of the deceased person or their family members specifically.
3. The PDPL, as amended, applies to data controllers within the KSA, but includes a broader mandate for entities outside the KSA that process data of KSA residents, regardless of specific criteria like offering goods or services or monitoring behavior.
4. The PDPL, as amended, applies to non-KSA entities that process the personal data of KSA residents.

1.2. Territorial scope

FAIRLY CONSISTENT

Both the GDPR and the PDPL, as amended, apply to organizations that have presence in the relevant jurisdictions and have extraterritorial scope.

However, on the one hand, the extraterritorial scope of the PDPL, as amended, is broader than the extraterritorial scope of the GDPR, considering that the former does not require offering goods or services or monitoring behavior to apply to a party outside the KSA processing data of individuals residing in the KSA.

On the other hand, the extraterritorial scope of the PDPL, as amended, applies to data subjects residing in KSA rather than the GDPR, which applies to data subjects that are located in the EU.

Similarities

GDPR

Articles 3(1) and (2)

1. The GDPR applies to organizations that have presence in the EU. In particular, Article 3(1) of the GDPR applies to entities or organizations 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.

2. The GDPR has extraterritorial effect.

PDPL, as amended

Article 2(1) of the PDPL, as amended

1. The PDPL, as amended, applies to organizations that have presence in the KSA. In particular, Article 2(1) of the PDPL, as amended, applies to any processing of personal data related to individuals that takes place in the KSA by any means.

2. The PDPL, as amended, has extraterritorial effect.

Differences

1. 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 behavior of individuals in the EU. The extraterritorial scope of the GDPR applies to the offering of goods or services to and/or the monitoring of behavior of individuals who are located in the EU, irrespective of residency and nationality.

1. In relation to extraterritorial scope, the PDPL, as amended, applies to any party outside the KSA that processes personal data of individuals residing in the KSA. The extraterritorial scope of the PDPL, as amended, therefore applies to KSA residents. Non-residents appear not to be covered.

1.3. Material scope

FAIRLY CONSISTENT

The GDPR and the PDPL, as amended, have a similar material scope of application, applying to the processing of personal data, which excludes processing of personal data for personal or household (family use) purposes.

However, the material scope of the PDPL, as amended, is broader than the material scope of the GDPR, considering that the former applies to manual and automated processing, regardless of whether the data is part of a filing system.

Similarities

GDPR

Articles 2-4, 9, and 26

Recitals 15-21, and 26

1. The GDPR applies to the 'processing' of personal data. The definition of 'processing' covers 'any operation' performed on personal data 'such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.'
2. The GDPR defines 'personal data' as 'any information' that directly or indirectly relates to an identified or identifiable individual.
3. 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.

PDPL, as amended

Articles 1, 2, and 27 of the PDPL, as amended

Article 9 of the Implementing Regulations

1. The PDPL, as amended, applies to the 'processing' of personal data. The definition of 'processing' covers 'any operation carried out on personal data by any means, whether manual or automated, including collecting, recording, saving, indexing, organizing, formatting, storing, modifying, updating, consolidating, retrieving, using, disclosing, transmitting, publishing, sharing, linking, blocking, erasing, and destroying data.'
2. The PDPL, as amended, defines 'personal data' as 'any data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual.
3. The PDPL, as amended, defines special categories of personal data as 'sensitive data' revealing racial or ethnic origin, or religious, intellectual, or political belief, data relating to security criminal convictions and offenses, biometric or genetic data for the purpose of identifying the person, health data, and data that indicates that one or both of the individual's parents are unknown. The PDPL, as amended, also provides specific requirements for the processing of special categories of personal data.

4. 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.'

5. The GDPR provides requirements for specific processing situations including processing for journalistic purposes and academic, artistic, or literary expression.

6. 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.

4. The PDPL, as amended, excludes from its application an individual's personal data processing for purposes that do not go beyond personal or family use, as long as the data subject did not publish or disclose it to others.

5. The PDPL, as amended, provides requirements for specific processing situations including processing for scientific, research, or statistical purposes.

6. The PDPL, as amended, excludes anonymized data from its application. Anonymized data is defined as data where both direct and indirect identifiers have been removed, making it permanently impossible to identify the data subject. Once anonymization is complete, the data is no longer considered personal data under the PDPL, as amended.

Differences

1. The GDPR does not apply to the personal data of deceased persons.

2. 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.

3. The GDPR does not provide specific requirements for controller anonymizing personal data.

1. The PDPL, as amended, applies to the data of deceased persons if it would lead to them or a member of their family being identified specifically.

2. The PDPL, as amended, applies to the processing of personal data within the KSA, including manual and automated processing, regardless of whether the data is part of a filing system.

3. The PDPL, as amended, provides specific requirements for controllers anonymizing personal data, such as evaluating the effectiveness of techniques applied by the controller for anonymizing personal data.

4. The GDPR excludes from its application data processing in the context of law enforcement or national security.

4. The PDPL, as amended, allows data processing in the context of law enforcement or national security.

2.1. Personal data

FAIRLY CONSISTENT

Both the GDPR and the PDPL, as amended, provide close definitions of personal data and special categories of data (sensitive data). In addition, both legislations provide definitions of health data (data concerning health) and genetic data.

Notably, while the PDPL, as amended, contains examples of personal data, it does not mention 'online identifiers' as provided for in the GDPR.

Similarities

GDPR

Articles 4(1) and 9
Recitals 26-30

1. 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.'
2. 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 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.'
3. The GDPR does not apply to 'anonymized' data, where the data can no longer be used to identify the data subject.

PDPL, as amended

Articles 1(4), 1(11)-1(13), and 1(15) of the PDPL, as amended
Article 9 of the Implementing Regulations

1. The PDPL, as amended, defines 'personal data' as any data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual, including name, personal identification number, addresses, contact numbers, license numbers, records, personal assets, bank and credit card numbers, photos and videos of an individual, and any other data of personal nature.
2. The PDPL, as amended, defines sensitive data as personal data revealing racial or ethnic origin, or religious, intellectual, or political belief, data relating to security criminal convictions and offenses, biometric or genetic data for the purpose of identifying the person, health data, and data that indicates that one or both of the individual's parents are unknown.
3. The Implementing Regulations note that anonymized data shall not be considered personal data.

Differences

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

2. The GDPR does not contain an equivalent provision.

3. The GDPR does not apply to the data of deceased individuals, this being left to Member States to regulate.

1. The PDPL, as amended, does not explicitly mention online identifiers. However, the PDPL, as amended, includes in the definition of personal data personal identification numbers, records, and any other data of personal nature.

2. The PDPL, as amended, includes data that indicates that one or both of the individual's parents are unknown in the definition of sensitive data.

3. The PDPL, as amended, definition of personal data includes the data of deceased individuals if it could lead to the identification or that of their family members.

2.2. Pseudonymization

CONSISTENT

The GDPR and the Implementing Regulations both define pseudonymization in a similar way.

Additionally, while the GDPR includes a provision clarifying that pseudonymization falls within the scope of personal data, a similar provision is not present in the PDPL, as amended, or the Implementing Regulations. However, this is referenced in the Personal Data Protection Destruction, Anonymization, and Pseudonymization guideline issued by the Saudi Data & Artificial Intelligence Authority (SDAIA).

Similarities

GDPR

Articles 4 and 11
Recital 26

1. The GDPR defines pseudonymized data as ‘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 organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.’

PDPL, as amended

Articles 1(7), 20(4)(b), 30(3) of the Implementing Regulations
Article 1(4) of the PDPL, as amended
The Personal Data Destruction, Anonymization, and Pseudonymization Guideline issued in August 2024

1. The Implementing Regulations and the Personal Data Destruction, Anonymization, and Pseudonymization Guideline define ‘pseudonymization’ as ‘conversion of the main identifiers that indicate the identity of the data subject into codes that make it difficult to directly identify them without using additional data or information.’ The pseudonymized data or additional information should be kept separately, and appropriate technical and administrative controls should be implemented to ensure that they are not specifically linked to the data subject’s identity.

Differences

1. The GDPR recommends that 'In order to create incentives to apply pseudonymization when processing personal data, measures of pseudonymization should, whilst allowing general analysis, be possible within the same controller when that same controller has taken technical and organizational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately.'

2. The GDPR provides that 'personal data which have undergone pseudonymization, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.'

1. While neither the PDPL, as amended, nor the Implementing Regulations contain a similar provision, Article 20(4)(b) of the Implementing Regulations provides pseudonymization as a security measure in processing activities.

2. While neither the PDPL, as amended, nor the Implementing Regulations contain a similar provision, the definition of 'personal data' under the PDPL, as amended, includes any data that may directly or indirectly make it possible to identify an individual. Additionally, the Personal Data Destruction, Anonymization, and Pseudonymization Guideline does set out that 'pseudonymized data is considered personal data because it may be used, in one way or another, to identify a specific individual.'

2.3. Controllers and processors



FAIRLY CONSISTENT

Both the GDPR and the PDPL, as amended, align on their definitions of controllers and processors, as well as regarding the controllers' obligations to maintain records and ensure that sufficient guarantees for the protection of personal data are provided, including in relation to contracting with processors.

The PDPL, as amended, does differ in that it does not require a representative be assigned within Saudi Arabia.

Similarities

GDPR

Articles 4, 17, 28, 30, 32, 33, 35, 37, and 38
Recitals 64, 90, and 93

1. 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.
2. A data processor is a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.
3. Data controllers must comply with the purpose limitation and accuracy principles and rectify a data subject's personal data if it is inaccurate or incomplete.

PDPL, as amended

Articles 1, 11(1), 14, 19, 20, 22, and 31 of the PDPL, as amended
Articles 17, 25, and 32 of the Implementing Regulations

1. The PDPL, as amended, defines a controller as any public entity, natural person, or private legal person that specifies the purpose and manner of processing personal data, whether the data is processed by that controller or by the processor.
2. The PDPL, as amended, defines a processor as any public entity, natural person, or private legal person that processes personal data for the benefit and on behalf of the controller.
3. Controllers can only collect personal data for purposes directly related to the controller and take sufficient steps to verify the accuracy, completeness, timeliness of the data, and relevance in relation to the purpose of collection.

4. Data controllers must implement technical and organizational security measures and notify supervisory authorities of data breaches.

5. The GDPR stipulates that data controllers and data processors keep records of processing activities and provides an exception from this obligation for small organizations. It also provides for the designation of a data protection officer (DPO) by data controllers or data processors.

6. The GDPR provides that where processing is carried out on behalf of a controller, the controller shall use only data processors providing sufficient guarantees to implement appropriate technical and organizational 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. In addition, the data processor shall not engage another data processor without prior specific or general written authorization of the controller.

7. The GDPR provides that a data controller or data processors conduct DPIAs in certain circumstances.

4. Controllers must implement all necessary organizational, administrative, and technical measures to protect personal data. Controllers should also notify SDAIA of data breaches.

5. Controllers should maintain records of the personal data processing activities, based on the nature of the activity carried out by the controllers. The newly issued Rules for Appointing a Data Protection Officer by SDAIA provides for the cases in which controllers and processors shall appoint a DPO.

6. The PDPL, as amended, provides that controllers shall only select processors providing the necessary guarantees to implement the provisions of the PDPL, as amended, and the Implementing Regulations. Controllers shall also monitor the compliance of said processors with the provisions of the PDPL, as amended, and the Implementing Regulations. The Implementing Regulations also provide for the obligations of processors in relation to engaging with a sub-processor, including the obligation of processors to receive prior approval from the controller.

7. The PDPL, as amended, states that controllers must conduct an impact assessment of personal data processing, based on the nature of the activity carried out by the controller, in accordance with the requirements set out in the Implementing Regulations.

Differences

1. 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.

1. The PDPL, as amended, does not require foreign controllers to appoint a representative within Saudi Arabia. However, the Implementing Regulations establish that when engaging with a processor, controllers should include in the contract clarifications of whether the processor is subject to regulations in other countries and the impact on their compliance with the PDPL, as amended, and its Regulations.

2.4. Children

FAIRLY INCONSISTENT

Both the GDPR and PDPL, as amended, provide that the consent of a legal guardian is required to process the personal information of children. Unlike the GDPR, the PDPL, as amended, and the Implementing Regulations do not explicitly mention children - only a data subject 'that fully or partially lacks legal capacity' - and do not contain provisions specifically targeted at protecting the personal information of children. However, the non-binding Elaboration and Developing Privacy Policy Guideline, issued by SDAIA in August 2024, provides some clarity on drafting privacy policies when processing personal data of children.

Similarities

GDPR

Articles 6, 8, 12, 40, and 57
Recitals 38, 58, and 75

1. The GDPR does not define 'child' nor 'children.'
2. 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.

PDPL, as amended

Articles 3(3), 4(7), 11, and 13 of the Implementing Regulations

1. The PDPL, as amended, does not define 'child' nor 'children.'
2. Under the Implementing Regulations, the controller must provide the required information in an appropriate language when aware that the data subject fully or partially lacks legal capacity. The non-binding Elaboration and Developing Privacy Policy Guideline issued by SDAIA in August 2024 clarifies that the privacy policy shall be designed in a clear and understandable manner for specific groups, including children, if the entity aims, in full or in part, to process data of such specific groups.

Differences

1. 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.

2. 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.

3. The GDPR provides that data controllers are required to make reasonable efforts to verify that consent is given or authorized by a parent or guardian.

4. The GDPR applies to information services.

5. The GDPR does not expressly foresee the prohibition for the controller to cause harm to the interest of a data subject and the requirement to enable the exercise of rights once legal capacity is reached.

1. The PDPL, as amended, and the Implementing Regulations do not foresee specific consent requirements for providing information society services to children. The PDPL, as amended, provides that the controller may not disclose personal data if the disclosure contradicts the interests of 'a person that fully or partially lacks legal capacity.'

2. The Implementing Regulations provide that the legal guardian of the person who fully or partially lacks legal capacity must act in their best interests and exercise their data subject rights, and consent to the processing of their personal data.

3. The Implementing Regulations conditions consent of the legal guardian upon taking appropriate measures to verify the validity of guardianship over the data subject.

4. The PDPL, as amended, does not explicitly refer to information services.

5. Under the Implementing Regulations, when obtaining consent from the legal guardian, the controller must not cause any harm to the interests of the data subject and must enable the exercise of rights by the data subject when they reach legal capacity.

2.5. Research

FAIRLY INCONSISTENT

Although both the GDPR and the PDPL, as amended, provide for the possibility of processing personal data for research purposes, the PDPL, as amended, imposes specific conditions for this type of processing.

The PDPL, as amended, also lacks particular provisions on the interpretation of scientific research and on data subject rights in the context of processing data for such purposes. However, both pieces of legislation provide for similar safeguards for using personal data for scientific research purposes.

Similarities

GDPR

Articles 5(1)(b), 9(2)(j), 14(5), 17(3), 21(6), and 89
Recitals 33, and 159-161

1. 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 minimization, and anonymization, etc.). 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.

PDPL, as amended

Article 27 of the PDPL, as amended
Article 30 of the Implementing Regulations

1. The Implementing Regulations set out additional controls for processing personal data for research purposes, as provided for in the PDPL, as amended. These controls include specifying a purpose, collecting personal data to the minimum extent necessary, and encoding personal data. The Implementing Regulations establish similar controls for processing personal data in the public interest.

Differences

1. 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

1. Under the PDPL, as amended, personal data may be collected or processed for scientific, research, or statistical purposes without the consent of the data subject if:
 - it does not specifically identify the data subject;
 - evidence of the data subject's identity will be

for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.’

2. 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.’

3. Under the GDPR, where personal data is 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.

4. 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.

destroyed during the processing and prior to disclosure of such data to any other entity, and if it is not sensitive data; or

- personal data collected or processed for these purposes is required by another law or in implementation of a previous agreement to which the data subject is a party.

2. The PDPL, as amended, does not define how scientific, research, or statistical purposes should be interpreted.

3. The PDPL, as amended, does not explicitly provide for derogations of data subject rights when the processing of personal data is for research purposes.

4. The PDPL, as amended, provides that personal data may be collected and processed for research purposes without the data subject’s consent, subject to the abovementioned conditions.

3. Legal basis

FAIRLY INCONSISTENT

Both the GDPR and the PDPL, as amended, include similar legal basis for data processing, although the 'legitimate interest' basis does not apply to sensitive data. Interestingly, unlike the GDPR, the PDPL, as amended, requires a legal basis for controllers to process data when collected from a source other than the data subject or when the processing relates to another purpose and for disclosures of personal data. These include the legal basis of processing publicly available data.

Similarities

GDPR

Articles 5-10

Recitals 39-48

1. 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; and
 - for the legitimate interest of the data controller when this does not override the fundamental rights of the data subject.
2. The GDPR recognizes consent as a legal basis to process personal data and includes specific information on how consent must be obtained and can be withdrawn.
3. Under the GDPR, as a general rule, the processing of special categories of personal data is restricted unless an exemption applies, which include the data subject's explicit consent.

PDPL, as amended

Articles 5, 6, 10, and 11 of the PDPL, as amended

Article 11 of the Implementing Regulations

1. The PDPL, as amended, requires the processing of personal data with the consent of data subjects unless exceptions apply, which include where:
 - processing is done in the implementation of a previous agreement to which the data subject is a party;
 - processing is pursuant to another law; or
 - processing is based on the legitimate interest of the controller, without prejudice to the rights and interests of the data subject, and provided that no sensitive data is processed.
2. The PDPL, as amended, and the Implementing Regulations recognize consent as a legal basis for data processing and include specific information on how consent must be obtained and withdrawn.
3. Under the Implementing Regulations, explicit consent must be obtained for processing sensitive data, credit data, or when decisions are made solely based on automated processing of personal data. The PDPL, as amended, and the Implementing Regulations contain further restrictions on processing sensitive data.

Differences

1. The GDPR provides the following grounds for processing:
 - to protect the vital interest of the data subject or of another natural person; or
 - for performance carried out in the public interest or in the official authority vested in the data controller.

2. The GDPR does not contain an equivalent provision. The GDPR establishes rules around the disclosure requirements where information is collected from the data subject.

3. The GDPR does not contain an equivalent provision. The legal bases for collecting personal data from the data subject and other sources are the same.

1. The PDPL, as amended, provides the following ground of processing, some of which are slightly different from the GDPR, and others which are not available under the GDPR:
 - when the processing serves the actual interests of data subject but communicating the same with the data subject is difficult or impossible; or
 - the controller is a public entity, and the processing is required for security purposes or to fulfil judicial requirements.

2. The PDPL, as amended, provides that the controller may only collect personal data directly from the data subject and may only process personal data for the purposes for which it has been collected.

3. The controller may collect personal data from a source other than the data subject and may process personal data for purposes other than the ones for which they have been collected in the following situations:
 - the data subject gives their consent;
 - personal data is publicly available or was collected from a publicly available source;
 - the controller is a public entity, and the collection or processing of the personal data is required for public interest or security purposes, to implement another law, or to fulfil judicial requirements;
 - complying with this may harm the data subject or affect their vital interests;
 - personal data collection or processing is necessary to protect public health, public safety, or to protect the life or health of specific individuals;
 - personal data is not to be recorded or stored in a form that makes it possible to directly or indirectly identify the data subject; or

- personal data collection is necessary to achieve legitimate interests of the controller, without prejudice to the rights and interests of the data subject, and provided that no sensitive data is to be processed.

4. The GDPR does not contain an equivalent provision. The GDPR establishes rules for data processing and does not distinguish legal bases based on collection and disclosure.

4. The controller may disclose personal data in the following situations:
- the data subject gives their consent to the disclosure;
 - personal data was collected from a publicly available source;
 - the entity requesting disclosure is a public entity, and the collection or processing of the personal data is required for public interest or security purposes, to implement another law, or to fulfil judicial requirements;
 - the disclosure is necessary to protect public health, public safety, or to protect the life or health of specific individuals;
 - the disclosure will only involve subsequent processing in a form that makes it possible to directly or indirectly identify the data subject; or
 - the disclosure is necessary to achieve legitimate interests of the controller, without prejudice to the rights and interests of the data subject, and provided that no sensitive data is to be processed.

5. The GDPR does not contain an equivalent provision. The GDPR establishes rules for data processing and does not distinguish legal bases based on collection and disclosure.

5. Restrictions to disclosures are further set out in Article 16, including where the disclosure results in violating the privacy of an individual other than the data subject.

4.1. Data transfers

FAIRLY CONSISTENT

Both the GDPR and the PDPL, as amended, allow cross-border data transfers subject to certain requirements being met. The structure and principles of the requirements are also similar.

However, the requirements of a lawful cross-border transfer under the PDPL, as amended, are stricter than the requirements set out in the GDPR, especially considering that exemptions to the requirements of an adequacy decision or appropriate safeguards are narrower than under the GDPR.

Similarities

GDPR

Articles 44-50

Recitals 101 and 112

PDPL, as amended

Article 29 of the PDPL, as amended

Articles 2-7 of the Regulation on Personal Data Transfer Outside the Kingdom (the Data Transfer Regulations)

1. The GDPR requires that personal data transferred internationally serves a legitimate and specific purpose. Under the GDPR, data transfers must align with the original processing purposes.
2. The GDPR allows transfers to countries recognized by the European Commission as providing adequate protection.
3. In the absence of an adequacy decision, the GDPR permits data transfers if appropriate safeguards are in place. The GDPR outlines mechanisms such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs).

1. The PDPL, as amended, mandates that data transfers outside the KSA must have a clear purpose, such as fulfilling obligations to which the data subject is a party or to perform necessary operations for central processing to enable the controller to conduct its activities.
2. The PDPL, as amended, as per the Data Transfer Regulations, permits transfers to countries that SDAIA deems to offer adequate protection.
3. In the absence of an adequacy decision, the PDPL, as amended, permits data transfers if appropriate safeguards are in place. The PDPL, as amended, outlines three mechanisms such as SCCs, BCRs, and certificate of accreditation.

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

5. The GDPR does not provide for any personal data localization requirements.

6. The EU SCCs contain a requirement for the data exporter to carry out a Transfer Impact Assessment (TIA). This assessment focuses on ensuring that the destination country provides a level of data protection that is 'essentially equivalent' to the EU, particularly in regard to government access and surveillance laws. The goal is to evaluate if any supplementary measures are needed to protect EU data subjects when data is transferred outside the EU.

7. The GDPR provides specific derogations that allow data transfers under certain conditions, such as the necessity of the transfer for important reasons of public interests.

4. The PDPL, as amended, specifies that a cross-border transfer is allowed based on international agreements for judicial cooperation.

5. The PDPL, as amended, does not provide for any personal data localization requirements. The PDPL, as amended, states that it will not prejudice laws that grant rights to data subjects or confer better protection to personal data, which may apply to laws containing data localization requirements.

6. The Data Transfer Regulations require controllers to conduct a risk assessment when implementing appropriate safeguards or when transferring sensitive data on a continuous or widespread basis. This assessment ensures that data transfers do not pose high risks to data subjects.

7. The PDPL, as amended, excludes from its data transfer requirements (other than needing a purpose for the transfer) cases of extreme necessity, including to protect the vital interests of the data subject and to prevent, examine, or treat a disease.

Differences

1. The GDPR provides specific derogations that allow data transfers under certain conditions, such as explicit consent from the data subject.
2. The GDPR does not have a specific provision related to data minimization for transfers. However, the GDPR generally requires that data processing comply with the principles of data minimization.
3. The GDPR does not contain limited exceptions from complying with the adequacy and data minimization rules.

1. The PDPL, as amended, does not contain specific derogations for data transfers, such as the data subject's explicit consent.
2. Transfers must be limited to the minimum amount of personal data necessary for the transfer (i.e., in compliance with the data minimization rules specified in the Implementing Regulations).
3. The PDPL, as amended, contains limited exemptions from complying with the adequacy and data minimization rules, although such exemptions may still require the application of safeguards such as SCCs. For example, controllers are exempt where the transfer or disclosure is non-recurring or for a limited period and involves a limited number of data subjects; although it requires the controller to comply with the SCCs or to ensure that the transfer is to a body that has received an approval certificate from an entity licensed by the competent authority and the data is not sensitive.

4.2. Data processing records

FAIRLY CONSISTENT

The GDPR and the PDPL, as amended, both require the maintenance of ROPA and establish similar ROPA obligations.

The obligation to keep ROPA under the PDPL, as amended, applies to all data controllers, but not to data processors, regardless of their size, while the GDPR requirements are limited by an organization's size in specific circumstances and apply to data processors as well as controllers.

Finally, the PDPL, as amended, requires ROPA to be retained for five years after the completion of the processing activity, whereas the GDPR is silent on the matter.

Similarities

GDPR

Article 30
Recital 82

PDPL, as amended

Article 31 of the PDPL, as amended
Article 33 of the Implementing Regulations

1. Controllers have an obligation to maintain a record of processing activities under their responsibility.
2. ROPA must include information such as:
 - the name and contact details of the controller and, where applicable, the DPO;
 - the purposes of data processing;
 - a description of the categories of data subjects and personal data;
 - the categories of recipients to whom personal data has been or will be disclosed;
 - details of any transfers of personal data to third countries or international organizations;
 - where possible, the envisaged time limits for erasure of different categories of data; and
 - where possible, a general description of the technical and organizational security measures in place.

1. Controllers must maintain records of their personal data processing activities based on the nature of the activity carried out by the controller.
2. The ROPA must include, as a minimum, information such as:
 - the controller's name and contact details;
 - where applicable, information about the DPO;
 - the purposes of personal data processing;
 - a description of the categories of personal data and data subjects;
 - the retention period for personal data and, where possible, specific retention periods for each category of personal data;
 - the categories of recipients to whom personal data has been or will be disclosed;
 - a description of data transfers outside Saudi Arabia, including the legal basis for the transfer and the recipients of the personal data; and
 - a description of the organizational, administrative, and technical measures in place to ensure the security of the personal data, where possible.

3. ROPA must be made available to the respective supervisory authorities upon request.

3. ROPA must be made available to SDAIA upon request.

Differences

1. The obligation to keep ROPA applies to data controllers and data processors.

1. The obligation to keep ROPA applies to data controllers only.

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

2. The obligation to keep ROPA applies to data controllers only.

3. Organizations with fewer than 250 employees are exempt from maintaining a ROPA unless their processing:
 - is not occasional;
 - is likely to result in a risk to the rights and freedoms of data subjects; or
 - involves special categories of data or data relating to criminal convictions and offenses.

3. The PDPL, as amended, does not provide exemptions based on organization size; all entities processing personal data are required to maintain a ROPA.

4. The GDPR does not specify a retention period for ROPA.

4. ROPA must be kept during the processing and for five years after the completion of the processing activity.

5. ROPA must be in writing or electronic form.

5. ROPA must be in writing.

4.3. Data Processing Impact Assessment



FAIRLY CONSISTENT

The GDPR and the PDPL, as amended, require the conducting of DPIAs in specified circumstances and detail information to be included in the assessment.

However, impact assessments under the PDPL, as amended, have a broader application than DPIAs under the GDPR, especially considering that the thresholds of risk triggering the requirement to conduct an impact assessment are lower under the PDPL, as amended.

Similarities

GDPR

Articles 35 and 36

Recitals 75, 84, and 89-93

PDPL, as amended

Article 22 of the PDPL, as amended

Article 25 of the Implementing Regulations

1. The GDPR requires controllers to complete a DPIA to identify and mitigate risks to data subjects when processing personal data in ways that may pose high risks to their rights and freedoms.
2. A DPIA must be conducted under specific circumstances where the processing is likely to result in high risk to data subjects.
3. A DPIA must include specific information such as:
 - a description of the processing activities and their purposes;
 - an assessment of the necessity and proportionality of the processing;
 - an evaluation of the risks to the rights and freedoms of data subjects; and
 - measures to address and mitigate those risks.

1. The PDPL, as amended, requires controllers to carry out a written and documented assessment of the potential impacts and risks that may affect data subjects as a result of personal data processing.
2. An impact assessment must be conducted under specific circumstances specified in the Implementing Regulations.
3. An impact assessment must include specific information such as:
 - the purposes and legal basis of processing;
 - a description of the nature of the processing, the types and sources of personal data processed, and recipients to whom personal data is disclosed;
 - a description of the scope of processing, which identifies the type of personal data and the geographical scope of the processing;
 - a description of the context of the processing, which identifies the relationship between the data subjects, controller(s), and processors, as well as any other relevant circumstances;

4. The GDPR requires DPIAs to be documented and retained as part of the organization's data protection compliance record.

- the necessity and proportionality of the measures to be taken to enable the controller and processor to process the minimal personal data necessary to achieve the purposes of processing;
- the impact of the processing, based on the severity of its impact, materially and morally, and the likelihood of any negative impact on data subjects, including any psychological, social, physical, or financial impact, and the likelihood of their occurrence;
- measures that will be taken to prevent or limit the risks; and
- the suitability of the measures envisaged to avoid identified risks.

4. The Implementing Regulations specify that the controller must prepare a written and documented assessment of the potential impacts and risks that may affect the data subject as a result of personal data processing.

Differences

1. The GDPR requires DPIAs for any processing that is 'likely to result in a high risk' to individuals' rights and freedoms, giving examples in guidelines but allowing some flexibility for organizations to determine if a DPIA is necessary. In particular, DPIAs are required where there is:
 - 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;
 - processing on a large scale of special categories of personal data or of personal data relating to criminal convictions and offenses; and
 - systematic monitoring of a publicly accessible area on a large scale.

1. The PDPL, as amended, specifies certain types of processing that automatically require an impact assessment, which adds more prescriptive guidance on when impact assessments are required. An impact assessment is required where:
 - there is processing of sensitive data;
 - there is collecting, comparing, or linking two or more sets of personal data obtained from different sources;
 - the activity of the controller includes on a continuous and large scale:
 - processing of personal data of those who fully or partially lack legal capacity;
 - processing operations that by their nature require continuous monitoring of data subjects;
 - processing personal data using new technologies; or

- making decisions based on automated processing of personal data; and
- a controller provides a product or service that involves processing personal data that is likely to cause serious harm to the privacy of data subjects.

2. These records should be available to supervisory authorities upon request.

3. 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.

4. The GDPR does not explicitly foresee cases where the DPIA must be provided to the controller's processors.

5. Where appropriate, controllers must seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

6. The GDPR does not explicitly foresee cases where the controller must reconduct the assessment due to an indication that the processing will harm the privacy of data subjects.

2. The PDPL, as amended, and the Implementing Regulations do not contain an equivalent provision.

3. The PDPL, as amended, and the Implementing Regulations do not explicitly foresee cases where the controller must consult the supervisory authority prior to any processing that would result in a high risk in the absence of risk mitigation.

4. The controller must provide a copy of the impact assessment to any processor acting on its behalf in relation to the relevant processing.

5. The PDPL, as amended, and the Implementing Regulations do not explicitly foresee cases where the controller must seek the views of the data subject.

6. The controller must - if the assessment indicates that the processing will harm the privacy of data subjects - address the reasons for that and reconduct the assessment.

4.4. Data protection officer appointment

FAIRLY CONSISTENT

The GDPR and the PDPL, as amended, both require the appointment of a DPO and outline similar obligations, including when a DPO must be appointed, professional qualities, and independence.

The circumstances requiring appointing a DPO under the PDPL, as amended, are broader than those set out in the GDPR, especially considering that there is no reference to large-scale volumes in case of processing of sensitive data. Furthermore, the PDPL, as amended, sets out vetting obligations concerning the appointment of DPO.

Similarities

GDPR

Articles 37-39

Recital 97

PDPL, as amended

Article 30 of the PDPL, as amended

Article 32 of the Implementing Regulations

The Rules for Appointing Personal Data Protection Officer

1. Under the GDPR, data controllers and data processors may be required to appoint a DPO. The DPO plays a central role in promoting data protection awareness, overseeing compliance, and serving as a contact point for supervisory authorities and data subjects.

1. Under the PDPL, as amended, a data controller may be required to appoint one or more individuals to be responsible for the protection of personal data.

2. The data controller must designate a DPO where:
 - the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
 - the core activities of a data controller or data processor consist of processing operations which, by virtue of their nature, scope, and/or purposes, require regular and 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, health information, and biometric data).

2. A data controller must appoint one or more individuals to be responsible for the protection of personal data in any of the following cases:
 - the controller is a public entity that provides services that involve the processing of personal data on a large scale;
 - the core activities of the controller consist of processing operations that require the regular and systematic monitoring of data subjects; and
 - the core activities of the controller consist of processing sensitive personal data (e.g., religious beliefs, ethnic origin, health information, and biometric data).

3. The controller must publish the contact details of the DPO and communicate them to the supervisory authority.

4. DPOs should operate independently, have adequate resources, and report to the highest management level. Controllers cannot assign tasks that may conflict with DPO tasks.

5. DPOs are responsible for monitoring data protection compliance and cooperating with supervisory authorities. They also serve as a point of contact for individuals to exercise their data protection rights.

6. The DPO must be designated on the basis of professional qualities and expert knowledge of data protection law and practices.

7. The DPO can be a staff member of the data controller or data processor or can perform tasks based on a service contract.

3. The data controller must provide SDAIA with the DPO's contact details immediately upon their appointment, through the National Data Governance Platform, and provide a clear and accessible means of communication with the DPO for data subjects.

4. DPOs should operate independently, have adequate resources, and report to the highest management level. Controllers cannot assign tasks that may conflict with DPO tasks.

5. DPOs are responsible for monitoring data protection compliance and cooperating with supervisory authorities. They also serve as a point of contact for individuals to exercise their data protection rights.

6. DPOs must have appropriate academic qualifications and experience in the field of personal data protection.

7. A DPO may be an executive, an employee of the controller, or an external contractor. Controllers must conclude an agreement with the external contractor when appointing a contractor outside the controller as a DPO.

Differences

1. Data processors must designate a DPO in specified circumstances.

2. A group of undertakings may appoint a single DPO provided that a DPO is easily accessible from each establishment.

1. The PDPL, as amended, only requires data controllers to appoint a DPO. However, when concluding an agreement between the controller and processor for processing personal data on behalf of the controller, the controller must verify whether the processor has a DPO. If the appointment of a DPO is required under the Rules for Appointing Personal Data Protection Officer, the controller should request the appointment to ensure that the necessary guarantees for implementing the provisions of the PDPL, as amended, and Implementing Regulations are in place.

2. The PDPL, as amended, does not explicitly address group undertakings.

4.5. Data security and data breaches



FAIRLY CONSISTENT

The GDPR and the PDPL, as amended, have similar obligations related to data security and data breaches including the requirement to adopt organizational and technical measures as well as to notify the supervisory authority of breaches in specific circumstances.

However, the circumstances triggering the obligation to notify the data subject in respect of the data breach under the PDPL, as amended, are broader than under the GDPR.

Similarities

GDPR

Articles 5, 24, and 32-34

Recitals 74-77 and 83-88

PDPL, as amended

Articles 19 and 20 of the PDPL, as amended

Articles 17, 23, and 24 of the Implementing Regulations
The Destruction, Anonymization, and Pseudonymization
Guideline

1. The GDPR recognizes 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.
2. The GDPR states that data controllers and data processors are required to implement appropriate technical and organizational security measures to ensure that the processing of personal data complies with the obligations of the GDPR.
3. 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.

1. The PDPL, as amended, recognizes the need for appropriate organizational, administrative, and technical measures to protect personal data, ensuring its security and confidentiality.
2. The PDPL, as amended, mandates that data controllers implement all necessary measures to protect personal data during processing and transmission to ensure that the processing of personal data complies with the obligations of the PDPL, as amended, including compliance with national cybersecurity standards or recognized best practices.
3. In case of a personal data breach, the controller must notify the competent authority when there is a breach or illegal access to personal data that could harm the data or cause prejudice to the data subject.

4. Under the GDPR, a personal data breach must be noticed to the supervisory authority without undue delay and, where feasible, no later than 72 hours after having become aware of the breach.

5. The GDPR provides a list of information that must be, at minimum, included in the notification of a personal data breach to supervisory authorities and to data subjects. For example, a notification must describe the nature of the breach, the consequences of the breach, and measures to mitigate possible adverse effects.

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

7. The GDPR provides a list of technical and organizational measures, where appropriate, that data controllers and data processors must implement such as pseudonymization, 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.

4. Under the PDPL, as amended, a personal data breach must be notified to the competent authority within 72 hours of becoming aware of a breach that could damage the personal data or that conflicts with the rights and interests of the data subject.

5. The PDPL, as amended, provides a list of information that must be, at minimum, included in the notification of a personal data breach to the competent authority and data subjects. For example, a notification must include a description of the breach, the risks, including the actual or potential impact on data subjects, and future measures taken to avoid the recurrence of a breach.

6. Processors must commit, in an agreement, to notify the controller in case of a personal data breach without undue delay in accordance with the provisions of the PDPL, as amended, and the Implementing Regulations.

7. The PDPL, as amended, generally requires that necessary organizational, administrative, and technical measures are taken to ensure the security of the personal data. Controllers must implement necessary security and technical measures to limit security risks to personal data breaches and comply with relevant controls, standards, and rules issued by the National Cybersecurity Authority (NCA) or recognized best practices and cybersecurity standards (if the controller is not obligated to follow the controls, standards, and rules of the NCA). Technical examples for destruction, pseudonymization and anonymization of personal data are set out in the Destruction, Anonymization, and Pseudonymization Guideline.

Differences

1. The controller must notify data subjects 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.

2. 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 organizational protective measures have been implemented;
- any subsequent measures have been taken in order to ensure that the risks are no longer likely to materialize; or
- it would involve disproportionate effort.

1. The controller must notify data subjects of a breach without undue delay if it could damage their data or impact their rights and interests, using simple and clear language.

2. The PDPL, as amended, does not explicitly provide for exemptions for notifying data subjects.

4.6. Accountability

 FAIRLY INCONSISTENT

In contrast to the GDPR, the PDPL, as amended, does not expressly set out accountability as a cornerstone principle of data processing, although it can be implied by means of other express obligations.

Similarities

GDPR

Articles 5(2), 24-25, 35, and 37
Recital 39

- 1. Not applicable.

PDPL, as amended

Articles 22, 30(2), and 31 of the PDPL, as amended
Articles 25, 32, and 33 of the Implementing Regulations

- 1. Not applicable.

Differences

- 1. The GDPR recognizes accountability as a fundamental principle of data protection. Controllers are responsible and must be able to demonstrate compliance with the data protection principles. Controllers must also implement ROPA, appoint a DPO in certain circumstances, and complete DPIAs where there is high risk processing.

- 1. Although the PDPL, as amended, does not expressly recognize accountability as a fundamental principle of data protection, it does set out several obligations requiring controllers to take responsibility for compliance with the PDPL, as amended, such as implementing ROPA, appointing a DPO under certain circumstances, and completing DPIAs in certain cases.

5.1. Right to erasure



FAIRLY CONSISTENT

Both the GDPR and the PDPL, as amended, have similar provisions relating to the right to erasure (or destruction). The laws also contain exceptions to the rights in similar situations, although the exceptions are not identical.

Similarities

GDPR

Articles 12 and 17

Recitals 59 and 65-66

PDPL, as amended

Articles 4(5), 11(4), 12, and 18 of the PDPL, as amended

Articles 3, 4, and 8 of the Implementing Regulations
Personal Data Destruction, Anonymization and
Pseudonymization Guideline

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

2. 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.'

3. 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.

4. 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.

1. Under the PDPL, as amended, data subjects have the right to request the deletion of their data when such data is no longer necessary for the purpose for which it was collected. The Implementing Regulations also provide that controllers must destroy personal data if the data subject withdraws their consent and consent was the sole legal basis for processing.

2. Controllers must act on data subject requests within a period not exceeding 30 days and without delay.

3. The PDPL, as amended, provides that controllers must use a privacy policy, which must specify information on data subject rights.

4. The Implementing Regulations provide that when destroying personal data, the controller must take appropriate measures to notify other parties and individuals to whom the controller disclosed personal data and request its destruction.

5. 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.

5. The Implementing Regulations provide that upon receiving a data subject request, controllers shall take appropriate measures to verify the identity of the requester before executing the request in accordance with relevant legal requirements.

Differences

1. The deadline for responding to a data subject request 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

1. The period for responding to a data subject request may be extended in case the implementation requires disproportionate effort, or if the controller receives multiple requests from the data subject, provided that the extension does not exceed an additional 30 days and the data subject is notified in advance of the extension with the reasons for the delay.

2. A request can be made in writing, orally, and through other means including electronic means, where appropriate.

2. Neither the PDPL, as amended, nor the Implementing Regulations describe how a data subject request can be made. However, the Implementing Regulations mention that controllers must take appropriate measures to document requests received, including oral requests.

3. This 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.

3. Neither the PDPL, as amended, nor its Executive Regulations discuss costs related to the right to exercise the right to deletion.

4. 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 defense of legal claims; and
 - complying with legal obligations for a public interest purpose.

4. Controllers may retain data after the purpose of the collection ceases to exist if:
 - the personal data does not contain anything that may lead to specifically identifying the data subject;
 - there is a legal basis for retaining the personal data for a specific period; or
 - the personal data is closely related to a case under consideration before a judicial authority and the retention of the personal data is required for that purpose.

5. The GDPR does not contain an equivalent provision.

5. The Implementing Regulations provide that when destroying personal data, controllers shall destroy all copies of the personal data stored in the controller's systems, including backups, in accordance with relevant regulatory requirements.

5.2. Right to be informed



FAIRLY CONSISTENT

The GDPR and the PDPL, as amended, accompanied by the Implementing Regulations, recognize a data subject's right to be informed and bear a significant amount of similarities. Both laws require data controllers to provide data subjects with information such as the details of the controller and the DPO, the purpose of processing, and the parties to whom personal data will be disclosed. Furthermore, both jurisdictions include specific provisions regarding processing for a different purpose, indirect collection, and time frames for communication.

However, unlike the PDPL, as amended, the GDPR explicitly allows for information to be communicated through various means (such as orally, in writing, or through electronic means); whereas the PDPL, as amended, requires for information to be provided through the use of a privacy policy.

Similarities

GDPR	PDPL, as amended
Articles 5-14 and 47	Articles 4(1), 12, and 13 of the PDPL, as amended
Recitals 58-63	Article 4 of the Implementing Regulations

1. Data subjects must be provided with information relating to the processing of personal data in order to validate their consent, including:
 - purposes of processing, including the legal basis for processing;
 - data subjects' rights (e.g., the right to erasure, right to object, right of withdrawal, right to lodge a complaint to a relevant authority, etc.);
 - the data retention period;
 - recipients or their categories of personal data;
 - the fact that the controller intends to transfer personal data to a third country or international organization; and
 - contact details of the data controller or its representative and the DPO.

2. 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.

1. The data subjects have the right to be informed on, among other things:
 - the legal basis and purpose of collecting personal data;
 - information on data subject rights and how to exercise them;
 - the period for which the personal data will be stored or, if that is not possible, the criteria used to determine that period;
 - the entities to which personal data will be disclosed;
 - whether the data will be transferred, disclosed, or processed outside the KSA; and
 - the controller's identity and contact details, as well as the contact details of the DPO, where applicable.

2. Under the Implementing Regulations, before conducting processing of personal data for another purpose than the one for which the data was collected, the controller must provide necessary information to the data subject.

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

4. 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.

5. In the case of indirect collection, a data controller must provide information relating to such collection to data subjects within a reasonable period after obtaining the data, but at the latest within one month, at the time of the first communication with the data subject, or when personal data is first disclosed to the recipient.

6. 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.

7. Data subjects must be informed of the existence of automated decision-making, including profiling, at the time when personal data is obtained.

8. The GDPR provides examples of circumstances, which can be considered 'legitimate interest.'

3. The PDPL, as amended, requires the controller to inform the data subject of the potential consequences and risks that may result from not collecting personal data.

4. Under the Implementing Regulations, in the case of indirect collection of personal data, the data subjects must be informed of the categories of personal data and the source from which the personal data was collected.

5. The Implementing Regulations require the controller, in the cases of indirect collection, to inform the data subject of information linked to such collection without undue delay and within a period not exceeding 30 days.

6. Under the PDPL, as amended, and the Implementing Regulations, information on processing must be provided to data subjects at the time of collection of their personal data from the data subject.

7. The Implementing Regulations require the controllers that make automated decisions based on personal data indicate to data subjects, among other things, whether decisions will be based solely on automated processing.

8. The Implementing Regulations provide legitimate interests include the disclosure of fraud operations and the protection of network and information security.

Differences

1. 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 electronic formats.

2. Information can be provided to data subjects orally, in addition to writing forms or electronic means.

3. A data controller must inform data subjects of the existence or absence of an adequacy decision, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

4. Where personal data is collected from the data subject, the controller must, at the time when personal data is obtained, provide the data subject with applicable information.

5. The GDPR does not contain an equivalent provision

1. Neither the PDPL, as amended, nor the Implementing Regulations explicitly provide format requirements. However the non-binding Elaboration and Developing Privacy Policy Guideline, issued by SDAIA in August 2024, includes a template privacy policy. Under the Implementing Regulations, the controller must provide the required information in appropriate language when aware that the data subject fully or partially lacks legal capacity.

2. Neither the PDPL, as amended, nor the Implementing Regulations explicitly outline if the information can be provided orally.

3. Neither the PDPL, as amended, nor the Implementing Regulations explicitly provide for a requirement to inform on transfers or adequacy decisions.

4. Information on processing must be provided to data subjects prior to, or at the time of, the collection of their personal data.

5. Controllers are required to provide confirmation that the personal data will not be subsequently processed in a manner inconsistent with the purpose.

5.3. Right to object

FAIRLY INCONSISTENT

The GDPR provides data subjects with the right to object to certain types of processing while the PDPL, as amended, does not. However, both the GDPR and the PDPL, as amended, provide for the right to withdraw consent at any time, including in relation to direct marketing, with similar consequences.

The PDPL, as amended, is more succinct in its provisions on the right to withdraw consent and establishes grounds for overriding data subjects' objection to the processing for marketing purposes.

Similarities

GDPR

Articles 7, 12, 18, and 21

1. Data subjects shall have the right to withdraw their consent to the processing of their personal data at any time.
2. Data subject must be informed of their right to withdraw consent.
3. A request to restrict the processing of personal data must be responded 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.

PDPL, as amended

Articles 5(2) and 25(2) of the PDPL, as amended
Articles 3(1), 4(1)(e), 8(1)(c), 12, and 29(3) of the Implementing Regulations

1. Data subjects may withdraw their consent at any time. The Implementing Regulations provide for further conditions.
2. Data subjects must be provided with an explanation of how to withdraw consent.
3. The Implementing Regulations provide that controllers have a period not exceeding 30 days to act on the data subject rights request including the right to obtain a restriction of processing when the accuracy is contested. This period may be extended for a period not exceeding 30 days, if acting on the request requires additional, unexpected, or unusual efforts or in the event that the controller receives multiple requests from the data subject.

Differences

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

2. Data subjects must be informed of information about how to exercise the right.

3. 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; or
- the processing of personal data is for scientific or historical research or statistical purposes.

4. 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 defense of a legal claim.

1. The PDPL, as amended, does not provide a right to object. However, the PDPL, as amended, states that consent can be withdrawn in relation to direct marketing. Individuals must also be provided with a mechanism to opt out of receiving advertising and awareness materials. In addition, the PDPL, as amended, provides an exemption for marketing related to awareness-raising materials sent by public entities.

2. The PDPL, as amended, does not provide a right to object.

3. The PDPL, as amended, does not provide a right to object.

4. The PDPL, as amended, does not provide a right to object.

5.4. Right to access



FAIRLY CONSISTENT

The GDPR, the PDPL, as amended, and the Implementing Regulations provide data subjects with the right of access. In addition, both the PDPL, as amended, and the GDPR contain restrictions on the right of access, including relating to national security and crime detection.

Similarities

GDPR

Articles 15 and 23

Recitals 59-64

PDPL, as amended

Articles 4(2), 4(3), 9, and 16 of the PDPL, as amended

Articles 3(1)(a), 3(1)(c), 3(2), 5, 6, and 10 of the Implementing Regulations

1. The GDPR recognizes that data subjects have the right to access their personal data that is processed by a data controller.
2. The GDPR provides that the right of access must not adversely affect the rights or freedoms of others.
3. The GDPR provides that the right of access must not adversely affect the rights or freedoms of others, including those related to trade secrets.
4. 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.

1. The PDPL, as amended, recognizes that data subjects have the right to access their personal data.
2. The PDPL, as amended, provides that the controller may limit the exercise of the right of access if necessary to protect the data subject or other parties from any harm.
3. The Implementing Regulations provide that exercising the right to access personal data should not negatively impact the rights of others, such as intellectual property rights or trade secrets.
4. The Implementing Regulations state that controllers must act on the request of the data subject for exercising their rights within a period not exceeding 30 days and without delay. This period may be extended by 30 days in case the implementation requires disproportionate effort, or if the controller receives multiple requests from the data subject.

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

6. The GDPR provides Member States to restrict the scope of the obligations and rights in relation to national security, defense, public security, protection of judicial independence and judicial proceedings, the protection of the data subject or the rights and freedoms of others, and the prevention, investigation, detection, or prosecution of criminal offenses.

5. The controller may refuse to act on request when it is repetitive, manifestly unfounded, or requires disproportionate efforts, in which case the data subject shall be notified of such reason.

6. The PDPL, as amended, provides additional grounds for refusal of the right to access, stating that the controller may limit the right of access in cases where the controller is a public entity and the restriction is required for security purposes, required by another law, or required to fulfil judicial requirements. Additionally, controllers may prevent data subject access to personal data if the disclosure:

- represents a threat to security, harms the reputation of the KSA, or conflicts with the interests of the KSA;
- prevents the detection of a crime, affects the rights of an accused to a fair trial, or affects the integrity of existing criminal procedures;
- compromises the safety of an individual; or
- results in violating the privacy of an individual other than the data subject, as set out in the Implementing Regulations.

Differences

1. 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 organizations;
- 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, 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 is not collected from the data subject, any available information as to their source; and
- the existence of automated decision-making, including profiling.

2. The GDPR does not contain an equivalent provision.

3. 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.

1. The PDPL, as amended, does not expressly outline the specific information to be provided in an access request but the right of access covers the personal data 'available to the controller.'

2. Controllers may prevent data subject access to personal data if, among others, the disclosure:

- conflicts with the interests of a person that fully or partially lacks legal capacity; or
- affects the KSA's relations with any other state.

3. Neither the PDPL, as amended, nor the Implementing Regulations provide information on whether fees can be charged. However, the template privacy policy set out in the non-binding Elaboration and Developing Privacy Policy Guideline, issued by SDAIA in August 2024, provides that data subjects shall not pay any fees for exercising their rights, unless otherwise provided by law.

4. 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.

4. The data subject shall have the choice to use one or many of the following means according to their preference considering options made available by the controller:

- email;
- text messages;
- the national address;
- communication via electronic applications; or
- any other communication means provided by the controller for this purpose.

In addition, the controller must provide access to personal data at a request from the data subject, or via a channel provided by the controller enabling the data subject to directly access their personal data without the need to make a request.

5.5 Right not to be subject to discrimination in the exercise of rights



CONSISTENT

Neither GDPR nor the PDPL, as amended, address the right not to be subject to discrimination in the exercise of rights.

Similarities

GDPR

- 1. The GDPR does not explicitly address the right not to be subject to discrimination.

PDPL, as amended

- 1. The PDPL, as amended, does not address the right not to be subject to discrimination.

Differences

- 1. Not applicable.

- 1. Not applicable.

5.6. Right to data portability

CONSISTENT

The PDPL, as amended, with the accompanying Implementing Regulations, provides data subjects with the right to request a copy of their personal data in a readable and clear format, similar to the right to portability under the GDPR. In particular, in both jurisdictions, the data subjects have the right to receive their personal data in a readable and electronic format.

Similarities

GDPR

Articles 12, 20, and 28

Recitals 68 and 73

1. The GDPR provides individuals with the right to data portability.
2. Anonymous data is not subject to the GDPR, and therefore, not subject to the right to data portability.
3. 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.'

PDPL, as amended

Article 4(3) of the PDPL, as amended

Article 6 of the Implementing Regulations

1. Under the PDPL, as amended, data subjects have the right to obtain their personal data held by the controller in a readable and clear format.
2. Under the Implementing Regulations, anonymized data is not considered personal data.
3. Under the Implementing Regulations, the data subject has the right to request a copy of their personal data in a readable and clear format. The personal data must be provided to the data subject in a commonly used electronic format, and the data subject may request a printed hard copy if feasible.

Differences

1. Under the right to data portability, the controller must transmit the data to another controller without hindrance.

2. The GDPR does not explicitly limit the right in this manner.

1. The PDPL, as amended, does not address the transmission of personal data to another controller.

2. The Implementing Regulations expressly foresee that exercising the right should not negatively impact the rights of others, such as intellectual property rights or trade secrets. Moreover, the controller must ensure that they do not disclose another individual's personal data when fulfilling the request.

6.1. Monetary penalties

FAIRLY INCONSISTENT

Both the GDPR and the PDPL, as amended, set out monetary penalties in case of breach of their data protection law. However, the PDPL, as amended, sets out fewer criteria to be considered when issuing a monetary penalty compared to the GDPR. Furthermore, the PDPL, as amended, provides that criminal sanctions may be applicable in addition to monetary penalties in limited circumstances.

Similarities

GDPR

Articles 83 and 84

Recitals 148-149

1. The GDPR provides for the possibility of administrative, monetary penalties issued by the supervisory authorities in cases of non-compliance.
2. When applying an administrative sanction, the supervisory authority must consider the nature, gravity, and duration of the infringement.

PDPL, as amended

Articles 35 and 36 of the PDPL, as amended

1. The PDPL, as amended, provides for the possibility of administrative, monetary penalties issued by the competent authority in cases of non-compliance.
2. Breaches shall be examined considering the type, gravity, and impact of the violation committed.

Differences

1. When applying an administrative sanction, the supervisory authority must consider:
 - 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;

1. The PDPL, as amended, does not establish equivalent factors.

- 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.

2. The GDPR does not provide for criminal sanctions.

2. On top of administrative and monetary penalties, the PDPL, as amended, provides criminal sanctions for breaches relating to sensitive data. The public prosecutor may punish by imprisonment for a term not exceeding two years, a fine of not more than SAR 3 million (approx. \$800,000), or both whoever discloses or publishes sensitive personal data in violation of the provisions of the PDPL, as amended, and if such act is with intent to harm the data subject or to achieve a personal benefit.

3. Depending on the violation occurred, the penalty may be up to either 2% of global annual turnover or €10 million, whichever is higher, or 4% of global annual turnover or €20 million, whichever is higher.

3. In circumstances where the above does not apply, the breach of any provision of the PDPL, as amended, may be punished by a warning or by a fine not exceeding SAR 5 million (approx. \$1.3 million). The above-mentioned fines may be doubled in case of recidivism, even if this results in exceeding their maximum limit, provided that they do not exceed double the limit.

4. Under the GDPR, it is left to Member States to create rules on the application of administrative fines to public authorities and bodies.

4. The PDPL, as amended, does not have an equivalent provision. However, the sanctions set out in the PDPL, as amended, are without prejudice to any more severe penalty provided for in another law.

6.2. Supervisory authorities



FAIRLY CONSISTENT

The GDPR and the PDPL, as amended, have similar provisions in respect to the powers of the competent supervisory authority, including investigatory and corrective powers.

However, the supervisory authority under the PDPL, as amended, is central, as opposed to multiple supervisory authorities under the GDPR competent for each EU Member State. Additionally, the financial structure and control mechanisms for the supervisory authority are not specified in the PDPL, as amended.

Similarities

GDPR

Articles 51-84

Recitals 117-140

PDPL, as amended

Articles 30 and 36 of the PDPL, as amended

1. Under the GDPR, supervisory authorities have investigatory powers which include:
 - ordering a controller and processor to provide information required;
 - conducting data protection audits;
 - carrying out a review of certifications issued; and
 - obtaining access to all personal data and to any premises.

2. Under the GDPR, supervisory authorities have corrective powers which includes imposing administrative fines.

1. Under the PDPL, as amended, the competent authority, SDAIA, has powers which include:
 - requesting the necessary documents or information from the controller to ensure compliance with the provisions of the PDPL, as amended, and the Implementing Regulations;
 - requesting the cooperation of any other party to support the enforcement of the PDPL, as amended, and the Implementing Regulations; and
 - specifying appropriate tools and mechanisms for monitoring controllers' compliance, including maintaining a national register of controllers.

2. Under the PDPL, as amended, SDAIA has corrective powers, which focus on imposing penalties and fines for violations of the law.

3. Under the GDPR, supervisory authorities shall also:
 - handle complaints lodged by data subjects; and
 - cooperate with data protection authorities from other countries.

4. Under the GDPR, supervisory authorities are tasked with promoting public awareness and the 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.

3. SDAIA shall:
 - handle complaints from data subjects regarding violations of the law; and
 - coordinate with other entities, such as the Central Bank and the Communications, Space & Technology Commission.

4. SDAIA shall, in coordination with relevant entities it deems appropriate, conduct an awareness campaign on an ongoing basis to inform data subjects, employees, or workers of controllers of the rights and duties contained in the PDPL, as amended.

Differences

1. Under the GDPR, supervisory authorities have corrective powers which include:
 - issuing warnings and reprimands;
 - imposing a temporary or definitive limitation including a ban on processing; and
 - ordering the rectification or erasure of personal data.

2. The GDPR does not explicitly provide the supervisory authorities with equivalent powers.

3. It is left to each Member State to establish a supervisory authority, and 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.

1. The PDPL, as amended, does not provide the supervisory authorities with equivalent powers.

2. Under the PDPL, as amended, SDAIA has powers which include providing services related to personal data protection through the national register or other appropriate means, with the possibility of collecting fees for these services.

3. Under the PDPL, as amended, there is a single competent authority designated by a resolution of the Council of Ministers. The PDPL, as amended, does not provide details about member qualifications, duration of terms, or reappointment conditions. Instead, SDAIA oversees data protection across Saudi Arabia without delegation to multiple supervisory bodies.

4. 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.

4. The financial structure and control mechanisms for SDAIA under the PDPL, as amended, are not specifically outlined, leaving room for potential government oversight without the explicit protections for independence seen in the GDPR.

6.3. Civil remedies for individuals, including other remedies



FAIRLY CONSISTENT

The GDPR and the PDPL, as amended, grant similar civil remedies to data subjects including a cause of action and the right to lodge a complaint.

However, under the PDPL, as amended, data controllers and data processors cannot exempt themselves from liability. Furthermore, data subjects must submit their claims within a defined time limit.

Similarities

GDPR

Articles 79, 80, and 82

Recitals 131, 146-147, and 149

1. 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.
2. 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 their complaint.

PDPL, as amended

Articles 34 and 40 of the PDPL, as amended

Article 37 of the Implementing Regulations

1. The PDPL, as amended, provides individuals with a cause of action to seek proportionate compensation for the material or moral damage caused by a violation of the PDPL, as amended, or its regulations.
2. The data subject has the right to submit any complaint that may arise out of the implementation of the PDPL, as amended, and its regulations to SDAIA.

Differences

1. 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.

1. The PDPL, as amended, does not contain a provision that provides a mechanism for data controllers or processors to exempt themselves from liability by proving that they are not at fault for an event that causes damage to the data subject.

2. 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 organization that has as its statutory objective the protection of data subject rights.

3. The GDPR does not explicitly impose a time limit for data subjects to submit complaints to supervisory authorities.

2. The PDPL, as amended, does not provide for collective redress mechanisms, meaning individuals that are data subjects generally have to file claims on their own rather than as part of a collective action or group litigation.

3. The PDPL, as amended, imposes a time limit to submit complaints to the competent authority. A data subject must submit a complaint within a maximum period of 90 days from the date of when the incident occurred or from that date of when the data subject became aware of it.

