Comparing privacy laws:
GDPR v. PDPL

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

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

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

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

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

Table of contents

Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') came into effect on 25 May 2018, and governs the protection of personal data in EU and EEA Member States. Saudi Arabia's first data protection law, namely the Personal Data Protection Law, implemented by Royal Decree M/19 of 17 September 2021 approving Resolution No.98 dated 14 September 2021 ('PDPL') (only available in Arabic here), was published in the Official Gazette on 24 September 2021 and take effect on 23 March 2022. Notably, the implementing decree of the law provides for an 18-month transition period for data controllers to achieve compliance from the date of its publication in the Official Gazette. However, this date may be delayed, as determined by the Saudi Data & Artificial Intelligence Authority ('SDAIA'), for a period of up to five years for companies located outside the Kingdom of Saudi Arabia that process personal data of Saudi Arabian residents.

The PDPL has many similarities with the GDPR and often uses the same general concepts as well as the same language on occasion, particularly with regards to data processing principles and data subject rights. While these foundations are largely mirrored between the two pieces of legislation, there are several key, nuanced differences. For instance, the PDPL provides less detailed information on the exercise of data subject rights, more restrictive data transfer obligations, as well as registration obligations on controllers. Notably, unlike the GDPR, the PDPL has less extensive principles and legal bases for processing personal data, with emphasis on consent as requirement for lawful processing. Furthermore, the PDPL notes throughout that the 'executive regulations' shall add further detail to various provisions of the PDPL.

Please note that the SDAIA issued, on 10 March 2022, in collaboration with the National Data Management Office ('NDMO'), the Draft Executive Regulations for the PDPL, and launched a public consultation on the same which ends on 25 March 2022. Once finalised, the executive regulations will be included within this comparison.

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

Structure and overview of the Guide

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

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

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

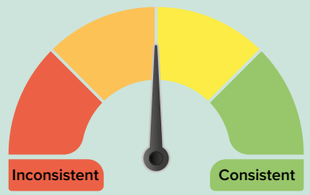
Key for giving the consistency rate

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

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

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

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



Usage of the Guide

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

1. Scope

1.1. Personal scope

The PDPL includes similar core concepts as the GDPR and refers to data controllers, data processors, and data subjects. Like the GDPR, the PDPL also includes public bodies within its scope. The GDPR and the PDPL differ, however, in that the latter does not refer to the nationality or place of residence of data subjects and does not exclude the personal data of deceased persons from its scope. Moreover, the definition of 'data subject' in the PDPL extends to the representative or legal guardian of the personal to whom the personal data relates.

	GDPR	PDPL
Data Controller	Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	Article 1(18): 'controlling entity' means any public entity, and natural or legal person, that determines the purposes and means of the processing of personal data, whether it processes the personal data itself or by means of another processing entity.
Data Processor	Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	Article 1(19): 'processing entity' means any public entity, and natural or legal person, that processes personal data for the benefit of, and on behalf of, the controlling entity.
Data Subject	Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Article 1(16): 'personal data owner' means the individual to whom the personal data relates to, his/her representative, or his/her legal guardian.
Public Bodies	Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body.	Article 1(71): Any ministry, department, public institution, public authority, or any independent public entity in the kingdom, or any of its affiliated entities.
Nationality of Data Subjects	Recital 14: The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.	Article 2(1): The PDPL applies to any processing of personal data related to individuals in the Kingdom by any means, including processing personal data related to individuals residing in the Kingdom by any means from any party outside the Kingdom.
Place of Residence	See Recital 14 above.	See Article 2(1) above.
Deceased Individuals	Recital 27: This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.	Article 2(1) of the PDPL expressly notes that it is applicable to the processing of personal data of a deceased person, if that personal data identifies the deceased or a member of their family.

1.2. Territorial scope

Fairly consistent

The GDPR establishes specific extraterritorial application for certain processing activities, while the PDPL establishes the same for entities processing personal data that relates to residents of Saudi Arabia.

	GDPR	PDPL
Establishment in Jurisdiction	Article 3: This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. Recital 22: Establishment implies the effective and real exercise of activity through stable arrangements.	Article 2(1): The PDPL applies to any processing of personal data related to individuals in the Kingdom by any means, including processing personal data related to individuals residing in the Kingdom by any means from any party outside the Kingdom, inclusive of personal data of deceased persons, if such data is capable of identifying him/her or a member of their family.
Extraterritorial	See Recital 22 above.	See Article 2(1) above.
Goods & Services from Abroad	Recital 23: In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.	The PDPL does not explicitly refer to goods and services from abroad.
Monitoring from Abroad	Recital 24: The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.	The PDPL does not explicitly refer to monitoring from abroad.

1.3. Material scope

Fairly consistent

The PDPL is generally similar to the GDPR in its material scope, and both apply to comparable concepts of personal data, data processing, special categories of data, and processing by automated or non-automated means. They are also both aligned in that they exempt the processing of personal data for personal use from their scope.

	GDPR	PDPL
Personal Data/ Personal Information	Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Article 1(4): 'personal data' means any information through which an individual may be directly or indirectly identified, including name, social security number, numbers, addresses, bank account and credit card details, and pictures. Article 2(1): 'personal data' includes the data of a deceased person, if such data would lead to his/her identification or a family member's identification
Data Processing	Article 4(2): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.	Article 1(5): 'processing' means any operation which is performed on personal data, whether manual or automated, including, collection, recording, keeping, indexing, arranging, formatting, storage, modification, updating, merging, retrieval, use, disclosure, transfer, publishing, sharing, blocking, erasure, or destruction.
Special Categories of Data	Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	Article 1(11): Personal data relating to a person's ethnic or tribal origin, or religious, intellectual, or political belief, or indicates his/her membership in non-governmental associations or institutions, as well as criminal and security data, biometric data, genetic data, credit data, health data, location data, and data that indicates a person's parent or parents are unknown.
Anonymised Data	Recital 26: The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	The PDPL does not explicitly refer to anonymised data.
Pseudonymised Data	Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	The PDPL does not explicitly refer to pseudonymised data.
Automated Processing	Article 2(1): This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.	Article 1(5): 'processing' means any operation which is performed on personal data, whether manual or automated, including, collection, recording, keeping, indexing, arranging, formatting, storage, modification, updating, merging, retrieval, use, disclosure, transfer, publishing, sharing, blocking, erasure, or destruction.
General Exemptions	Article 2(2): This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law; (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union; or (c) by a natural person in the course of a purely personal or household activity. [See also Recital 26, above]	Article 2(2): This law does not apply to the processing of personal data for personal or family use, as long as it is not shared and disclosed to others. [Note: Article 2(2) further provides that the meaning of 'personal use' and 'family use' shall be determined by the executive regulations to the PDPL.]

2. Key definitions

2.1. Personal data

Definitions under the PDPL are in close alignment with the those of the GDPR, however there are minor differences, particularly in relation to special categories of data e.g. the PDPL's reference to tribal origins, credit data, and data indicating whether an individual's parents are unknown.

	GDPR	PDPL
Personal Data/ Personal Information	Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Article 1(4): 'personal data' means any information through which an individual may be directly or indirectly identified, including name, social security number, numbers, addresses, bank account and credit card details, and pictures.
Special Categories of Data	Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	Article 1(11): Personal data relating to a person's ethnic or tribal origin, or religious, intellectual, or political belief, or indicates his/her membership in non-governmental associations or institutions, as well as criminal and security data, biometric data, genetic data, credit data, health data, location data, and data that indicates a person's parent or parents are unknown.
Online Identifiers	Recital 30: Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.	The PDPL does not explicitly refer to online identifiers.

2.2. Pseudonymisation

Unlike the GDPR, the PDPL does not make explicit reference to either anonymisation or pseudonymisation.

	GDPR	PDPL
Anonymisation	Recital 26: 'anonymous information' is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	The PDPL does not explicitly refer to anonymised data.
Pseudonymisation	Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	The PDPL does not explicitly refer to pseudonymised data, however Article 18(1) provides that: the controlling entity shall erase the personal data it possesses as soon as the purpose of its processing terminates, unless the personal data is kept in an anonymised form ensuring that data subjects cannot be identified in accordance with the controls specified by the Regulations.

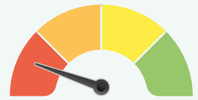
2.3. Controllers and processors

Fairly consistent

The definitions within the PDPL closely mirror those of the GDPR for data controllers, processors, Data Protection Impact Assessments ('DPIA'), and data protection officers ('DPO'), however the GDPR provides more details on requirements regarding controller and processor contracts.

	GDPR	PDPL
Data Controller	Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	Article 1(18): 'controlling entity' means any public entity, and natural or legal person, that determines the purposes and means of the processing of personal data, whether it processes the personal data itself or by means of another processing entity.
Data Processor	Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	Article 1(19): 'processing entity' means any public entity, and natural or legal person, that processes personal data for the benefit of, and on behalf of, the controlling entity.
Controller and Processor Contracts	Article 28(3): Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. [Article 28 goes on to stipulate necessary information to be included in such a contract.]	Article 8: Taking into account what the law and regulations stipulate regarding the disclosure of personal data, the controlling entity, when choosing a processing entity, must be committed to choose an entity that provides appropriate guarantees for the implementation of the provisions of the law and its executive regulations, and must continuously review the relevant entity's compliance with its instructions on all matters related to the protection of personal data, in a manner that does not conflict with the provisions of the law and the regulations, and without prejudice to its responsibilities towards the personal data owner or competent authority, as the case may be. The regulations shall set out the necessary provisions for this, including provisions relating to any subsequent contracts made by the processing entity.
Data Protection Impact Assessment ('DPIA')	DPIA is not specifically defined, however Article 35 sets out requirements for DPIAs (see section 4.3. for further information).	DPIA is not specifically defined, however Article 22 sets out a requirement for DPIAs (see section 4.3. for further information).
Data Protection Officer ('DPO')	DPO is not specifically defined, however Article 37 sets out requirements related to DPOs (see section 4.4. for further information).	DPO is not specifically defined, however Article 30 sets out requirements for related to DPOs (see section 4.4. for further information).

2.4. Children



Inconsistent

Unlike the GDPR, the PDPL does not refer to the offering of information society services directly to a child nor does it or provide an age threshold for processing data without the consent of the holder of parental responsibility.

	GDPR	PDPL
Children's Definition	The GDPR does not specifically define 'child'. However, Article 8(1) provides: Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.	The PDPL does not explicitly address children's data.
Consent for Processing Children's Data	Article 8(2): The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.	The PDPL does not explicitly provide for consent in relation to children's personal data, however Article 5 provides that: Except as stipulated by the law, personal data should not be processed, or the purposes of its processing changed, unless consent is obtained by its owner. The regulations shall set out the conditions of consent, when it must be in writing, and the terms and conditions related to obtaining the consent of a legal guardian, if the data subject does not have the capacity to do so.
Privacy Notice	Recital 58: Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.	Article 12: The controlling entity must put in place a personal data privacy policy and make it available to data subjects to review before collecting their data. The policy shall include the purpose of its collection, the categories of personal data collected, the means of collection, means of storage, processing, erasure, as well as data subject rights and how to exercise them.

2.5. Research

Both the GDPR and the PDPL provide for processing of personal data for research purposes, however each sets its own requirements and allowances with regards to processing personal data. In particular, the GDPR requires appropriate safeguards to be implemented for processing to take place while the PDPL provides for certain circumstances where personal data may be processed without the consent of the data subject.

	GDPR	PDPL
Scientific/ Historical Research Definition	Recital 159: Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. Recital 160: Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.	While the PDPL does not specifical define what is meant by scientific/historical research, Article 27 provides that: Personal data may be collected or processed for scientific, research, or statistical purposes, without the consent of its owner, in the following cases: • if the personal data does not specifically indicate the identity of the data subject; • if everything indicating the identity of the data subject specifically will be destroyed during its processing, and before disclosing it to any other party, and such data is not sensitive data; or • if the collection or processing of personal data for these purposes is required by another law or in implementation of an earlier agreement to which the data subject is a party.
Compatibility with Original Purpose of Collection	Article 5(1)(b): Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').	See Article 27 above. Article 5 provides that: Except as stipulated by the law, personal data should not be processed, or the purposes of its processing changed, unless consent is obtained by its owner [...]. Furthermore, Article 10 provides for specific circumstances where the controlling entity may collect personal data from other than its owner or process it for a purpose other than that for which it is collected. Article 11(1) provides that: the purpose of collecting personal data must be directly related to the stated purposes of the controlling entity and must not conflict with any provision of the law.
Appropriate Safeguards	Article 89(1): Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner.	The PDPL does not expressly address safeguards in relation to processing for scientific or historical research purposes.
Data Subject Rights (Research)	Under Article 17(3), the right to erasure may not apply in cases of scientific or historical research. Article 21(6), however, provides that data subjects may exercise the right to object to data processing for scientific or historical research purposes. In addition, Article 89 provides that Member States may derogate from the GDPR in regard to data subject rights and data processing for research purposes.	The PDPL does not expressly address processing for research purposes in relation to particular data subject rights.

3. Legal basis

While the GDPR provides for six legal grounds for processing personal data, the PDPL recognises consent as the main legal basis for data processing and provides for exceptions to consent in certain circumstances. In addition, the PDPL specifies several conditions for lawful processing of personal data that are in close alignment to those of the GDPR.

	GDPR	PDPL
Legal Grounds	Article 6(1): Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.	Article 5(1): Except for the cases stipulated in the PDPL, personal data may not be processed or the purpose of its processing changed without the consent of its owner. The regulations shall set out the conditions for consent, the conditions in which the consent must be in writing, and the terms and conditions for obtaining consent from the legal guardian if the personal data owner is incompetent or incompetent. Article 6: The processing of personal data is not subject to the consent in the following cases: (1) When the processing achieves a real interest for the data subject and contact with them is impossible or difficult to achieve; (2)When the processing is under another system or in implementation of a previous agreement to which the owner of the personal data is a party; and (3)If the controller is a public entity, and such processing is required for security purposes or to satisfy judicial requirements. Article 10: The controlling entity may collect personal data from its owner directly and that such data may only be processed to achieve the purpose for which it was collected. The controlling entity may however collect personal data from sources other than the data subject or process personal data for purposes other than those for which it was collected for in the following circumstances: • if the data subject agrees to this, in accordance with the provisions of the law; • if the personal data is publicly available, or if it was collected from a publicly available source; • if the controlling entity is a public entity, and the collection of personal data from other than its owner directly, or processing it for a purpose other than that for which it is collected, is required for security purposes, to implement another law, or to meet judicial requirements in accordance with the provisions set out by the regulations; if compliance with this prohibition may harm the data subject or affect his vital interests, in accordance with the provisions set out by the regulations; • if the collection or processing of personal data is necessary to protect public health or safety, or to protect the life or health of particular individual(s). The regulations set out the controls and procedures related thereof; and • if the personal data will not be recorded or kept in a form that makes it possible to identify or know its owner directly or indirectly. The regulations set out the controls and procedures related thereto. Article 11 further outlines conditions for lawful processing of personal data.

	GDPR	PDPL
Sensitive Data (Legal Basis)	There are specific requirements for processing special categories of data, see Article 9 of the GDPR for further information.	The PDPL does not provide for specific requirements for processing special categories of data
Conditions for Consent	Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. Article 4(11): 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.	Article 5(1): Except as provided for in the PDPL, personal data may not be processed, or the purposes changed, unless the consent of the concerned data subject is obtained. (2) In all cases, the data subject may withdraw his/her consent referred to in Article 5(1) at any time, and the regulations shall specify the relevant provisions thereof. Article 7: The consent referred to in Article 5(1) of the law may not be a condition for the provision of a service or benefit, unless the processing of personal data for which the consent is obtained is related to the service or benefit.
Journalism/ Artistic Purposes	Article 85(1): Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.	The PDPL does not expressly address journalism/artistic purposes.

4. Controller and processor obligations

4.1. Data transfers

The GDPR and PDPL differ in their data transfer requirements, with the PDPL adopting a restrictive starting point, prohibiting transfers of personal data outside Saudi Arabia. Notably, the supplementary regulations to the PDPL shall set out other purposes for which the transfer of personal data outside the Kingdom may be permitted, which may bring the law in closer alignment with the GDPR.

	GDPR	PDPL
Adequate Protection	Article 45(1): A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.	Article 29: Except in cases of extreme necessity relating to a threat to the life of the data subject, controllers may not transfer personal data outside the Kingdom unless the transfer is required to comply with an agreement to which the Kingdom is party, to serve Saudi interests, or for other purposes set out in the Regulations, provided that the following conditions set in Articles 29(1) to (4) are met: • the data transfer must not prejudice national security or the Kingdom's vital interests; • the transferring entity must provide adequate guarantees for protecting the personal data that will be transferred or disclosed and maintain its confidentiality, so that the data protection standards are not less than the standards stipulated in the PDPL and executive regulations; • the transfer must be restricted to the minimum personal data that is necessary for its purpose; and • the competent authority must approve the transfer. [Note: Article 29 further notes that except for the condition of Article 29(1), the competent authority can excuse a controller, on a case-by-case basis, from compliance with any of the other conditions in Article 29, if the competent authority itself or in cooperation with other bodies, assesses that the personal data will be accorded with sufficient safeguards outside the Kingdom and so long as no sensitive personal data is included.]
Other Mechanisms for Data Transfers	Article 46(1): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. (2) The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by: (a) a legally binding and enforceable instrument between public authorities or bodies; (b) binding corporate rules in accordance with Article 47; (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in	The PDPL does not explicitly refer to any other data transfer mechanisms. [Note: Article 29 provides that the regulations may set out further purposes for which data transfers outside the Kingdom may be permitted.]

	GDPR	PDPL
Other Mechanisms for Data Transfers (cont'd)	Article 93(2); (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2); (e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or (f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights. (3) Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by: (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.	
Data Localisation	Not applicable.	The PDPL does not explicitly refer to data localisation, however Article 29 provides for a restrictive approach to transferring data abroad.

4.2. Data processing records

The GDPR requires both controllers and processors to maintain data processing records, whereas the PDPL only explicitly outlines this obligation in relation to controllers. The GDPR also outlines more extensive requirements in relation to the information that should be included in processing records.

	GDPR	PDPL
Data Controller Obligation	Article 30(1): Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (f) where possible, the envisaged time limits for erasure of the different categories of data; and (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1)	Article 31: the controlling entity is required to keep records of its processing activities for a period determined by the Regulations depending on the nature of the processing activity, and available upon request by the competent authority, and shall as a minimum include the following: • contact details of the controlling entity; • the purpose of processing personal data; • a description of the categories of data subjects; • any party to which personal data has been, or will be, disclosed; • whether personal data has been, or will be, transferred outside the Kingdom or disclosed to a party outside the Kingdom; and • the period of time expected for keeping personal data.
Data Processor Obligation	Article 30(2): Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing: (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer; (b) the categories of processing carried out on behalf of each controller; (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; and (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).	The PDPL does not explicitly reference processing entities with regards to the record keeping obligation.
Records Format	Article 30(3): The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.	The PDPL does not explicitly refer to the format of records. However, Article 32(3) provides that: A special record shall be allocated in the portal for each controlling entity in which the records referred to in Article 31 of the law and other necessary documents or information related to the processing of personal data shall be recorded.
Required to Make Available	Article 30(4): The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.	Article 31: the controlling entity shall make personal data processing records available to the competent authority when requested.

	GDPR	PDPL
Exemptions	Article 30(5): The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.	The PDPL does not explicitly refer to any exemptions in relation to record of personal data activities.
General Data Processing Notification ('DPN')	Not applicable.	Article 32(1): The competent authority shall establish an electronic portal for the purpose of building a national record of controlling entities, which aims to monitor and follow up on the compliance of these entities with the provisions of the law and the regulations, [...]. (2) All controlling entities are required to register in the portal referred to in Article 32(1), and the competent authority shall collect a fixed annual fee, not exceeding SAR 100,000 (approx. €22,800) for registration of controlling entities [...].

4.3. Data protection impact assessment

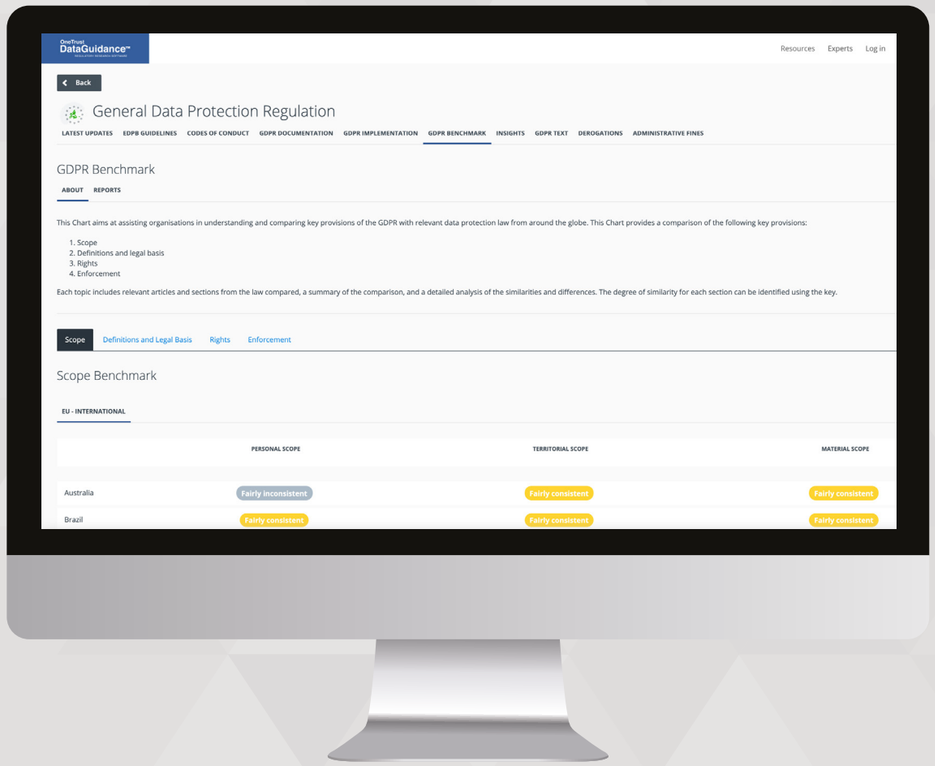
The DPIA requirements under the GDPR are similar to those of the PDPL, although the former is more detailed in relation to the content and manner of carrying out DPIAs. However, further details in relation to the PDPL may be provided by the executive regulations once issued.

	GDPR	PDPL
When is a DPIA Required	Article 35(1): Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. [...] (3) A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale.	Article 22: The controlling entity shall conduct an assessment of the consequences of processing personal data for their processing activities according to the nature of the controlling entity's processing activity, and the Regulations shall specify the necessary provisions thereof
DPIA Content Requirements	Article 35(7): The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.	The PDPL does not explicitly refer to any content requirements, however Article 22 provides that the regulations shall specify the necessary provisions relating to the obligation.
Consultation with Authority	Article 36(1): The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. [Article 36 goes on to detail requirements related to such prior consultation].	The PDPL does not explicitly require consultation with the competent authority.

Global Regulatory Research Software

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

Monitor regulatory developments, mitigate risk, and achieve global compliance



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

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

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

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

- Scope
- Rights
- Definitions and legal basis
- Enforcement

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

OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

Start your free trial at
www.dataguidance.com

4.4. Data protection officer appointment

Fairly consistent

The DPO requirements under the GDPR are similar to those of the PDPL, although the GDPR is more detailed and sets out a list of tasks to be undertaken by the DPO as well as notification requirements. Further details in relation to the PDPL may be provided by the executive regulations once issued.

	GDPR	PDPL
DPO Tasks	Article 39(1): The data protection officer shall have at least the following tasks: (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; (d) to cooperate with the supervisory authority; and (e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.	The PDPL does not make express reference to DPO tasks, however Article 30(2) provides that the Regulations shall set out further provisions relating to the appointment of a DPO.
When is a DPO Required	Article 37(1): The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.	Article 30(2): The controlling entity shall appoint or designate one or more persons to be responsible for implementing the provisions of the law and the Regulations. The Regulations shall set out the provisions thereof. Notably, Article 33(2) provides that controlling entities that operate outside the Kingdom and process personal data of Saudi citizens must appoint a representative in the Kingdom that the competent authority can resort to regarding compliance with the applicable laws.
Group Appointments	Article 37(2): A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.	The PDPL does not explicitly reference group appointments.
Notification of DPO	Article 37(7): The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.	The PDPL does not explicitly provide for notification of DPOs.
Qualifications	Article 37(5): The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.	The PDPL does not specify DPO qualifications.

4.5. Data security and data breaches

Fairly consistent

While there are several similarities between the PDPL and the GDPR, the PDPL does not clarify exceptions from breach notification requirements or processor notification requirements, is less clear in its definitions of security measures, and seems to provide for a shorter timeframe for breach notifications.

	GDPR	PDPL
Security Measures Defined	Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	Article 19: The controlling entity shall take the necessary organisational, administrative, and technical measures and means to ensure the preservation of personal data, including when it is transferred, in accordance with the provisions and controls specific by the regulations. [Note: the implementing decree to the PDPL notes that the competent authority, when preparing the regulations supplementing the PDPL, should consider establishing provisions and conditions relating to the technical and organisational measures attached to how personal data is kept by controllers, which should include the measures to safeguard personal data depending on its nature and sensitivity.]
Data Breach Notification to Authority	Article 33(1): In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.	Article 20(1): The controlling entity shall notify the competent authority as soon as it becomes aware of a data security breach.
Timeframe for Breach Notification	See Article 33(1) above.	See Article 20(1) above.
Notifying Data Subjects of Data Breach	Article 34(1): When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.	Article 20(2): The regulations shall determine in which circumstances controllers must inform data subjects of a security breach of their personal data. However, where such a breach may cause serious harm to the individual or their personal data, controllers must inform them immediately of the breach.
Data Processor Notification of Data Breach	Article 33(2): The processor shall notify the controller without undue delay after becoming aware of a personal data breach.	The PDPL does not provide for processor notification of data breaches.
Exceptions	Article 34(3): The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that	The PDPL does not specify exceptions to the breach notification requirement.

	GDPR	PDPL
Exemptions (cont'd)	the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.	

4.6. Accountability

The GDPR specifically provides for the principle of accountability and detailed obligations regarding the liability of controllers and processors, while the PDPL does not.

	GDPR	PDPL
Principle of Accountability	Article 5(2): The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability'). [Paragraph 1 details principles of: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality.]	The PDPL does not explicitly provide for the principle of accountability, however, the implementing decree to the PDPL provides that controlling entities shall take the necessary measures to hold work sessions and the like for its employees or workers, to introduce the terms and principles contained in the law after its entry into force [...].
Liability of Data Controllers and Data Processors	Article 82 (2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.	Article 40: Without prejudice to the imposition of penalties stipulated in the law, damages are available to data subjects for material and non-material loss in relation to breaches of any provisions of the law and/or the Regulations.

5. Rights

5.1. Right to erasure

Both the GDPR and the PDPL provide for the right to erasure. However, the GDPR provides additional legal grounds for exercising the right, as well as additional exceptions. The GDPR also provides more detail than the PDPL in relation to fees, timeframes, and the format of the response.

	GDPR	PDPL
Grounds for Erasure	Article 17(1): The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).	Article 4: Data subjects, subject to the provisions of the law, have the following rights: [...](4) the right to request the erasure personal data in possession of the controlling entity once the purposes for collecting the data have been exhausted and without prejudice to Article 18.
Inform Data Subject of Right	Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.	Article 12: The controlling entity must put in place a personal data privacy policy and make it available to data subjects to review before collecting their data. The policy shall include the purpose of its collection, the categories of personal data collected, the means of collection, means of storage, processing, erasure, as well as data subject rights and how to exercise them.
Fees	Article 12(5): Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.	Article 21: The controlling entity shall respond to the requests of data subjects regarding their rights under the law within the period determined, and through the means set out, by the regulations.
Response Timeframe	Article 12(3): The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the	See Article 21 above.

	GDPR	PDPL
Response Timeframe (cont'd)	data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.	
Format of Response	Article 12(1): The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.	See Article 21 above.
Publicly Available Data	Article 17(2): Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.	The PDPL does not explicitly refer to publicly available data.
Exceptions	Article 17(3): Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims. Article 12(5): Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.	Article 4(4) provides that the right to erasure applies without prejudice to Article 18. Article 18(1): The controlling entity shall erase the personal data it possesses as soon as the purpose of its processing terminates, unless the personal data is kept in an anonymised form ensuring that data subjects cannot be identified in accordance with the controls specified by the Regulations. Article 18(2): The controlling entity shall keep the personal data even after the purpose of its collection has ceased in the following cases: • if there is a legal justification that requires keeping it for a specific period, and in this case it shall be erased after the end of this period, or the purpose of its collection, whichever is longer; or • if the personal data is closely related to a case pending before a judicial authority, and it is required to be kept for this purpose, and in this case it shall be destroyed after completion of the judicial procedures related to the case.

5.2. Right to be informed

Fairly consistent

Both the GDPR and the PDPL provide for the right to be informed. However, the GDPR provides additional requirements as to what information needs to be provided to data subjects and makes a distinction between personal data obtained directly from the data subject and personal data obtained from a third party. The GDPR also provides additional requirements on intelligibility, and format requirements, as well as exceptions.

	GDPR	PDPL
Informed Prior to/at Collection	Article 13(1): Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. (2) In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (d) the right to lodge a complaint with a supervisory authority; (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	Article 4: Data subjects, subject to the provisions of the law, have the following rights: (1) the right to be informed, and that includes informing the data subject of the legal or practical justification for the collection of the data, the purpose thereof, and that the data should not be processed at a later date in a manner inconsistent with the purposes for which it was collected or in a manner otherwise than as stipulated in Article 10 of the law.
What Information is to be Provided	See Article 13(1) and (2) above.	See Article 4(1) above.
When Data is from Third Party	In addition to the information required under Article 13, Article 14(2) replaces the requirement that data subjects are provided with information on the legitimate interests pursued by the controller or by a third party, with an obligation to inform data subjects of the categories of personal data. Furthermore, paragraph (e) of Article 13(2) is replaced with a requirement to inform data subjects of the source from which the personal data originate, and if applicable, whether it came from publicly accessible sources.	The PDPL does not explicitly address situations where data is obtained from a third party.
Intelligibility Requirements	Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.	Article 21: The controlling entity shall respond to the requests of data subjects regarding their rights under the law within the period determined, and through the means set out, by the regulations.
Format	See Article 12(1) above.	See Article 21 above.
Exceptions	The requirements of Article 13 do not apply where the data subject already has the information. The requirements of Article 14 do not apply where: (a) the data subject already has the information; (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available; (c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.	The PDPL does not explicitly refer to any exceptions to the right to be informed.

5.3. Right to object

Unlike the GDPR, the PDPL does not provide for the right to object to processing of personal data.

	GDPR	PDPL
Grounds for Right to Object/Opt Out	Article 21(1): The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.	The PDPL does not explicitly provide for the right to object to the processing of personal data.
Withdraw Consent	Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.	Article 5(2): In all cases, the data subject may withdraw the consent referred to in Article 5(1) of the PDPL at any time, and the regulations specify the appropriate procedure thereof.
Restrict Processing	Article 18(1): The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.	The PDPL does not explicitly provide for the right to restrict processing of personal data.
Object to Direct Marketing	Article 21(3): Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.	The PDPL does not provide for the right to object to direct marketing.
Inform Data Subject of Right	See Article 12(1) in section 5.1. above. In addition, Article 21(4) provides: At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.	The PDPL does not explicitly provide for the right to object to the processing of personal data.
Fees	See Article 12(5) in section 5.1. above.	The PDPL does not explicitly provide for the right to object to the processing of personal data.
Response Timeframe	See Article 12(3) in section 5.1. above.	The PDPL does not explicitly provide for the right to object to the processing of personal data.
Format of Response	See Article 12(1) in section 5.1. above.	The PDPL does not explicitly provide for the right to object to the processing of personal data.
Exceptions	See Article 12(5) in section 5.1. above.	The PDPL does not explicitly provide for the right to object to the processing of personal data.

5.4. Right of access

Both the GDPR and the PDPL provide for the right of access to personal data. However the PDPL provides less detail with regards to the information to be provide to data subjects in connection with exercising their right to access.

	GDPR	PDPL
Grounds for Right of Access	Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.	Article 4: Data subjects, subject to the provisions of the law, have the following rights: [...](2) The right to access to his/her personal data that the controlling entity possesses, which includes accessing it, and obtaining a copy thereof, in a clear format that is identical to the content of the records and free of charge, as determined by the Regulations, without prejudice to the stipulations of the Credit Information Law regarding financial consideration, and without prejudice to Article 9 of the PDPL.
Information to be Accessed	Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; and (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	See Article 4(2) above.
Inform Data Subject of Right	See Article 12(1) in section 5.1.	Article 12: The controlling entity must put in place a personal data privacy policy and make it available to data subjects to review before collecting their data. The policy shall include the purpose of its collection, the categories of personal data collected, the means of collection, means of storage, processing, erasure, as well as data subject rights and how to exercise them.
Fees	See Article 12(5) in section 5.1. above.	See Article 4(2) above.
Verify Data Subject Request	Recital 64: The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.	The PDPL does not explicitly refer to verification of data subject requests.

	GDPR	PDPL
Response Timeframe	See Article 12(3) in section 5.1. above.	Article 21: The controlling entity shall respond to the requests of data subjects regarding their rights under the law within the period determined, and through the means set out, by the Regulations.
Format of Response	See Article 12(1) in section 5.1. above.	See Articles 4(2) and 21 above.
Exceptions	See Article 12(5) in section 5.1. above.	The PDPL does not explicitly refer to any exceptions to the right of access.

5.5. Right not to be subject to discrimination

Neither the GDPR, or the PDPL explicitly outline a right not to be subject to discrimination. However, the GDPR does provide for the right not to be subject to a decision based solely on automated processing.

	GDPR	PDPL
Definition of Right	The GDPR only implies this right and does not provide an explicit definition for it.	The PDPL does not explicitly provide for the right not to be subject to discrimination.
Automated Processing	Article 22(1): The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. [Article 22 goes on to detail this right, including exceptions]	The PDPL does not explicitly refer to data subject rights in relation to automated processing.

5.6. Right to data portability

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

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

6. Enforcement

6.1. Monetary penalties

Despite both the GDPR and the PDPL providing for monetary penalties, the PDPL provides a maximum penalty of SAR 5 million (approx. €1,211,390), where the GDPR adopts a two-tier approach with regard to percentages of annual turnover or a fine of up to €20 million, whichever if higher. Notably, the PDPL sets out that the relevant court may also order confiscation of funds gained as a result of violations of the law and/or require publication of the judgment at the offender's expense.

	GDPR	PDPL
Provides for Monetary Penalties	The GDPR provides for monetary penalties.	The PDPL provides for monetary penalties.
Issued by	Article 58(2) Each supervisory authority shall have all of the following corrective powers: [...] (i): to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.	Article 35(2): The Public Prosecution is responsible for investigating and prosecuting before the competent court for the violations stipulated in this Article. (3) The competent court shall hear cases arising from the application of this Article and impose the prescribed penalties. Article 36(2): The chairman of the competent authority shall form one or more committee(s) with no less than three members, one of whom shall be designated as the leader, and one as a legal or regulatory advisor, to take over inspection of violations and impose the relevant penalty warning or fine in accordance with Article 36(1) of the PDPL, according to the type of violation committed, its seriousness, and the extent of its consequences [...].
Fine Maximum	Article 83(5): infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to €20 million, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; (b) the data subjects' rights pursuant to Articles 12 to 22; (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49; (d) any obligations pursuant to Member State law adopted under Chapter IX; (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1). (6) Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to €20 million, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.	Article 35(1): Without prejudice to a more severe penalty in another law, the penalty for committing the following violations shall be stated opposite to them: (a) the penalty in relation to disclosure or publication of sensitive personal data may include imprisonment for up to two years and/or a fine not exceeding SAR 3 million (approx. €726,000); and (b) The penalty in relation to violations of the data transfer provision in Article 29 of the PDPL may result in imprisonment for up to one year and/or a fine not exceeding SAR 1 million (approx. €242,000). Article 36(1): [...] For violations of other provisions of the PDPL, penalties are limited to a warning notice or a fine not exceeding SAR 5 million (approx. €1,211,390). [Note: Fines may be increased to up to double the stated maximums for repeat offences.]
Percentage of Turnover	Under Article 83(4), (5), and (6), fines may be issued that equate to 2% or 4% of the total worldwide annual turnover of the preceding financial year.	Not applicable.
Mitigating Factors	Article 83(2): When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following: (a) the nature, gravity and duration of the infringement taking into	The PDPL does not explicitly provide for mitigating factors.

	GDPR	PDPL
Mitigating Factors (cont'd)	account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; (b) the intentional or negligent character of the infringement; (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects; (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32; (e) any relevant previous infringements by the controller or processor; (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; (g) the categories of personal data affected by the infringement; (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement; (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures; (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and (k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.	
Imprisonment	Not applicable.	See Articles 35 and 36 above.
DPO Liability	Not applicable.	Not applicable.

6.2. Supervisory authority

Both the GDPR and the PDPL provide for a data protection authority to give effect to the respective data protection laws, however the GDPR provides more detail and specifies the powers and tasks thereof.

Notably, the implementing decree includes specific provisions regarding the data protection authority's cooperation and coordination with other authorities such as the Communications Information Technology Commission and the Saudi Central Bank, calling for the preparation of memorandums of understanding to regulate coordination between the authorities.

	GDPR	PDPL
Provides for Data Protection Authority	Article 51(1): Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').	The implementing decree to the PDPL provides that the SDAIA shall be the competent authority, for a period of two years, during which consideration shall be given, in light of the results of the application of the provisions of the PDPL and its regulations and in light of the level of maturity in the data sector, to transfer the supervisory role to the NDMO.
Investigatory Powers	Article 58(1): Each supervisory authority shall have all of the following investigative powers: (a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks; (b) to carry out investigations in the form of data protection audits; (c) to carry out a review on certifications issued pursuant to Article 42(7); (d) to notify the controller or the processor of an alleged infringement of this Regulation; (e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks; (f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.	The PDPL does not explicitly refer to investigatory powers of the supervisory authority.
Corrective Powers	Article 58(2): Each supervisory authority shall have all of the following corrective powers: (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation; (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation; (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation; (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period; (e) to order the controller to communicate a personal data breach to the data subject; (f) to impose a temporary or definitive limitation including a ban on processing; (g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19; (h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met; (i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending	The PDPL does not explicitly refer to corrective powers of the supervisory authority.

	GDPR	PDPL
Corrective Powers (cont'd)	on the circumstances of each individual case; (j) to order the suspension of data flows to a recipient in a third country or to an international organisation.	
Authorisation/ Advisory Powers	Article 58(3): Each supervisory authority shall have all of the following authorisation and advisory powers: (a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36; (b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data; (c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation; (d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5); (e) to accredit certification bodies pursuant to Article 43; (f) to issue certifications and approve criteria of certification in accordance with Article 42(5); (g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2); (h) to authorise contractual clauses referred to in point (a) of Article 46(3); (i) to authorise administrative arrangements referred to in point (b) of Article 46(3); (j) to approve binding corporate rules pursuant to Article 47.	The implementing decree to the PDPL provides that the competent authority shall, in coordination with such authorities it deems appropriate, conduct a continuous awareness campaign for personal data owners, as well as for the employees of the controlling entities or their employees, to clarify the rights and obligations contained in the PDPL after its entry into force.
Tasks of Authority	Article 57(1): Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: (a) monitor and enforce the application of this Regulation; (b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention; (c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing; (d) promote the awareness of controllers and processors of their obligations under this Regulation; (e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end; (f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary; (g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation; (h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority; (i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices; (j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2); (k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4); (l) give advice on the processing operations referred to in Article 36(2); (m) encourage	The implementing decree to the PDPL provides that:[...] Sixth: The competent authority shall coordinate with the Saudi Central Bank to prepare a Memorandum of Understanding to regulate aspects related to the application of the provisions of the Law and its Regulations in the entities subject to the regulatory supervision of the Saudi Central Bank, to determine the role of each, so that competencies do not overlap, and to maintain the independence of the Saudi Central Bank [...], and the preparation of the memorandum should be completed and signed concurrently with the entry into force of the Law. Seventh: the competent authority shall cooperate with the Communications and Information Technology Commission to prepare a Memorandum of Understanding to regulate some aspects related to the application of the provisions of the Law and its Regulations in the entities subject to the Regulation of the Communications and Information Technology Commission, and to prevent any impact on the Communications and Information Technology Commission's role as an independent regulatory authority that supervises sensitive sectors related to the personal transactions of individuals, and to enhance the stability and growth of the sectors it supervises, and the memorandum should be completed and signed concurrently with the entry into force of the Law. Eighth: The competent authority shall, in coordination with such authorities it deems appropriate, conduct a continuous awareness campaign for personal data owners, as well as for the employees of the controlling entities, or their employees, to clarify the rights and obligations contained in the Law after its entry into force. Tenth: The competent authority shall, in coordination with the relevant authorities it deems appropriate, evaluate the results of the application of the Law and provide relevant feedback, including

	GDPR	PDPL
Tasks of Authority (cont'd)	the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5); (n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5); (o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7); (p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43; (q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43; (r) authorise contractual clauses and provisions referred to in Article 46(3); (s) approve binding corporate rules pursuant to Article 47; (t) contribute to the activities of the Board; (u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and (v) fulfil any other tasks related to the protection of personal data.	proposing any necessary amendments, within five years from the date of its entry into force, and submitting the necessary recommendations for completing the required actions. Eleventh: The competent authority shall, within a period not exceeding one year from the date of entry into force of the Law, and in coordination such relevant authorities as it deems appropriate, review the provisions of the relevant laws, decisions, and regulations that deal with provisions related to the protection of personal data of individuals, propose amendments thereto in accordance with the provisions of the Law, and submit recommendations on aspects regarding which legal actions are required to be completed. Twelfth: The competent authority shall, when preparing the Regulations of the Law, take into account the development of provisions and controls related to the organisational, administrative, and technical procedures and means related to storing personal data with the controlling entities in a manner that ensures the preservation of personal data according to its nature and degree of sensitivity, based on the provisions of Article 19 of the Law.
Annual Report	Article 59: Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.	The PDPL does not make explicit reference to annual reports.

6.3. Civil remedies for individuals

Both the GDPR and the PDPL provide civil remedies for data subjects, however the GDPR additional provisions on data subject representation for lodging complaints, processor liability, and exceptions to liability.

	GDPR	PDPL
Provides for Claims/Cause of Action	Article 79: Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.	Article 34: The data subject may file any complaint arising from the application of the Law and the Regulations with the competent authority. The Regulations specify the controls for the competent authority's handling of complaints filed by data subjects.
Material and Non-Material Damage	Article 82(1): Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.	Article 40: Without prejudice to the imposition of penalties stipulated in the law, damages are available to data subjects for material and non-material loss in relation to breaches of any provisions of the law and/or the Regulations.
Mandate for Representation	Article 80(1): The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.	The PDPL does not explicitly refer to representation.
Specifies Amount for Damages	Not applicable.	Not applicable.
Processor Liability	Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.	The PDPL does not explicitly mention processor liability.
Exceptions	Article 82(3): A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.	The PDPL does not explicitly refer to exceptions from liability.