Comparing privacy laws:
GDPR v. DIFC Law 2007 and 2020

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

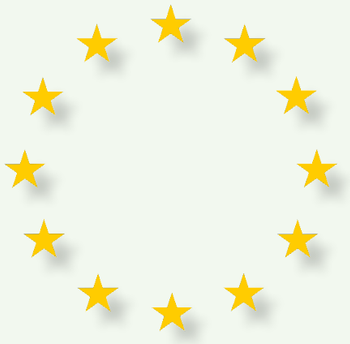
OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

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: LysenkoAlexander / Essentials collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com
Icon p.33-40: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.47-51: cnythzl / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com

Table of contents



Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') came into effect on 25 May 2018, and governs the protection of personal data in EU and EEA Member States. The Dubai International Financial Centre ('DIFC') enacted, on 1 June 2020, the Data Protection Law DIFC Law No.5 of 2020 ('the DIFC Law 2020') and the Data Protection Regulations 2020 ('the Regulations 2020'). These replaced the Data Protection Law 2007 DIFC Law No. 1 of 2007 ('the DIFC Law 2007') and the Data Protection Regulations ('the DPR 2018') respectively. The DIFC Law 2020 was enacted with a grace period and came into full effect on 1 October 2020.

Notably, the DIFC has published proposed amendments to the DIFC Law 2020, which were been subject to a public consultation on 25 February 2021, Consultation Paper No. 2 of 2021 on Proposed Amendments to the Data Protection Law No. 5 of 2020 ('the Draft Amendments'). At present, the Draft Amendments have not enacted into law yet.

The DIFC Law 2020 is significantly influenced by international standards for data protection such as the GDPR and CCPA, and seeks to move DIFC privacy legislation into closer alignment with these. While its core is similar to the DIFC Law 2007, there are several new obligations for data controllers and data processors as well as extensive clarifications of key requirements. For example, the DIFC Law 2020 introduces new data subject rights, such as the right to data portability or the right to object to automated decision-making, as well as defining what should be included in controller to processor agreements and the regulation of sub-processors. Furthermore, the DIFC Law 2020 contains provisions that in some ways extend beyond the GDPR by providing more nuanced requirements, such as that data protection officers ('DPOs') conduct annual assessments. Elsewhere, the DIFC Law 2020 remains less comprehensive than the GDPR and most notably in a more restricted territorial scope. In general terms, though, the DIFC Law 2020 will move data protection requirements much closer to the obligations provided under the GDPR.

The overview organises provisions from the GDPR, the DIFC Law 2020, and the DIFC Law 2007 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 the DIFC Law 2007 and 2020.

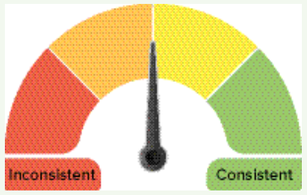
Key for giving the consistency rate

Consistent: The GDPR and the DIFC Law 2007 and 2020 bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.

Fairly consistent: The GDPR and the DIFC Law 2007 and 2020 bear a high degree of similarity in the rationale, core, and the scope of the provision considered, however, the details governing its application differ.

Fairly inconsistent: The GDPR and the DIFC Law 2007 and 2020 bear several differences with regard to the scope and application of the provision considered, however, its rationale and core presents some similarities.

Inconsistent: The GDPR and the DIFC Law 2007 and 2020 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

Consistency with the DIFC Law 2020: Fairly Consistent

Consistency with the DIFC Law 2007: Fairly Consistent

The DIFC Law 2020 does not differ from the DIFC Law 2007 in regard to this topic.

The DIFC Law 2020 employs similar core concepts as the GDPR and refers to data controllers, data processors, and data subjects. Like the GDPR, the DIFC Law 2020 also includes public bodies within its scope and excludes deceased individuals. The GDPR and the DIFC Law 2020 differ, however, in that the latter does not refer to the nationality or place of residence of data subjects.

GDPR	DIFC Law 2020	DIFC Law 2007
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.	Schedule 1.3: 'controller' means any person who alone or jointly with others determines the purposes and means of the processing of personal data.	Schedule 1.3: 'data controller': Any person in the DIFC who alone or jointly with others determines the purposes and means of the processing of personal data.
Data Processor		
Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	Schedule 1.3: 'processor' means any person who processes personal data on behalf of a controller.	Schedule 1.3: data processor: any person who processes personal data on behalf of a data controller.
Data Subject		
Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Schedule 1.3: 'data subject' means the identified or identifiable natural person to whom personal data relates. Schedule 1.3: 'Iidentifiable natural person' means a natural living person 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 (1) or more factors specific to his biological, physical, biometric, physiological, mental, genetic, economic, cultural or social identity (and 'Identified Natural Person' is interpreted accordingly).	Schedule 1.3: identifiable natural person: is a natural living person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his biological, physical, biometric, physiological, mental, economic, cultural or social identity.

GDPR	DIFC Law 2020	DIFC Law 2007
Public Bodies		
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body.	Schedule 1.1: a 'person' includes any natural person, body corporate or body unincorporate, including a company, partnership, unincorporated association, government or state.	Schedule 1.1(1)(b): a person includes any natural person, body corporate or body unincorporate, including a company, partnership, unincorporated association, government or state.
Nationality of Data Subject		
Recital 14: The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.	The DIFC Law 2020 does not refer to the nationality of data subjects.	The DIFC Law 2007 does not refer to the nationality of data subjects.
Place of Residence		
Recital 27: This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.	The definition of an identifiable natural person, see Schedule 1.3 of the DIFC Law 2020 above, explicitly defines applicable 'persons' as 'living'.	The definition of an identifiable natural person, see Schedule 1.3 of the DIFC Law 2007 above, explicitly defines applicable 'persons' as 'living'.

1.2. Territorial scope

The DIFC Law 2020 establishes notably more detailed provisions regarding its territorial scope compared to the DIFC Law 2007.

Unlike the GDPR, the DIFC Law 2020 does not establish a specific extraterritorial application for certain processing activities, although it does provide that it applies to any processing activity in the DIFC. This includes where the controller or processor is not incorporated within the DIFC but the processing is part of stable arrangements within the DIFC.

GDPR	DIFC Law 2020	DIFC Law 2007
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 6: (1) This Law applies in the jurisdiction of the DIFC. [...] (3) This Law applies as follows: (a) This Law applies to the processing of personal data by a controller or processor incorporated in the DIFC, regardless of whether the processing takes place in the DIFC or not. (b) This Law applies to a controller or processor, regardless of its place of incorporation, that processes personal data in the DIFC as part of stable arrangements, other than on an occasional basis. This Law applies to such controller or processor in the context of its processing activity in the DIFC (and not in a third country), including transfers of personal data out of the DIFC. (c) For the purposes of this Article 6(3), processing 'in the DIFC' occurs when the means or personnel used to conduct the processing activity are physically located in the DIFC, and processing 'outside the DIFC' is to be interpreted accordingly.	Article 5: This Law applies in the jurisdiction of the Dubai International Financial Centre. [Note: Schedule 1.1(3) specifies 'references in this Law to a body corporate include a body corporate incorporated outside DIFC.' A 'body corporate' may be a 'person'. In turn, a data controller may be 'any person in the DIFC'.]

GDPR	DIFC Law 2020	DIFC Law 2007
Extraterritorial		
See Recital 22, above.	See Article 6(3) above.	Article 5: This Law applies in the jurisdiction of the Dubai International Financial Centre.
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 DIFC Law 2020 does not explicitly refer to goods and services from abroad.	The DIFC Law 2007 does not refer to goods and services from abroad.
Monitoring from Abroad		
Recital 24: The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.	The DIFC Law 2020 does not explicitly refer to monitoring from abroad.	The DIFC Law 2007 does not refer to monitoring from abroad.

1.3. Material scope

While the general concepts of personal data and data processing remain the same from the DIFC Law 2007, the DIFC Law 2020 also specifies matters related to anonymisation, pseudonymisation, and automated processing in more detail.

The DIFC Law 2020 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. There are variations, though, in relation to anonymisation, pseudonymisation, and general exemptions.

GDPR	DIFC Law 2020	DIFC Law 2007
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.	Schedule 1.3: 'personal data' means any information referring to an identified or identifiable natural person. Schedule 1.3: 'Identifiable natural person' means a natural living person 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 his biological, physical, biometric, physiological, mental, genetic, economic, cultural or social identity (and 'Identified Natural Person' is interpreted accordingly).	Schedule 1.3: personal data: any data referring to an identifiable natural person. Schedule 1.3: 'Identifiable natural person': is a natural living person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his biological, physical, biometric, physiological, mental, economic, cultural or social identity.
Data Processing		
Article 4(2): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.	Schedule 1.3: process, processed, processes and processing (and other variants) means any operation or set of operations performed upon personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage and archiving, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, transfer or otherwise making available, alignment or combination, restricting (meaning the marking of stored personal data with the aim of limiting processing of it in the future), erasure or destruction, but excluding operations or sets of operations performed on personal data by:	Schedule 1.3: process, processed, processes and processing: any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

GDPR	DIFC Law 2020	DIFC Law 2007
Data Processing (cont'd)		
	(a) a natural person in the course of a purely personal or household activity that has no connection to a commercial purpose; or (b) law enforcement authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security.	
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.	Schedule 1.3: personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person. [Note: Part 2B specifies additional requirements for processing special categories of data].	Schedule 1.3: personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life.
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.	Although the DIFC Law 2020 does not specifically refer to its applicability in relation to anonymised or pseudonymised data, it refers to both in Article 22. Specifically, Article 22 provides that where processing must cease personal data should be deleted, anonymised, pseudonymised, or securely encrypted, among other measures.	The DIFC Law 2007 does not refer to anonymised data. However, Article 8(1)(e) requires that data controllers ensure that the personal data which they process is 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data was collected or for which they are further processed'.

GDPR	DIFC Law 2020	DIFC Law 2007
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.	Although the DIFC Law 2020 does not explicitly refer to its applicability in relation to anonymised or pseudonymised data, it refers to both in Article 22. Specifically, Article 22 provides that where processing must cease personal data should be deleted, anonymised, pseudonymised, or securely encrypted, among other measures.	The DIFC Law 2007 does not 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 6(2): This Law applies to the processing of personal data: (a) by automated means; and (b) other than by automated means where the personal data forms part of a filing system or is intended to form part of a filing system.	The definition of processing under the DIFC Law 2007 clarifies that processing may or may not be by automatic means.
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 65(1): The DIFCA Board of Directors may make Regulations exempting controllers from compliance with this Law or any parts of this Law. Such Regulations shall be consistent with the principles contained within this Article. [Note: Article 65 goes on to detail exemptions for official DIFC bodies.]	Section 39: (1) The DIFCA Board of Directors may make Regulations exempting data controllers from compliance with this Law or any parts of this Law. (2) Without limiting the generality of Article 39(1), Articles 11,12 13, 14 and 17 and 18 shall not apply to the DFSA [Dubai Financial Services Authority], DIFCA [Dubai International Financial Centre Authority] and the Registrar if the application of these Articles would be likely to prejudice the proper discharge by those entities of their powers and functions under any laws administered by the DFSA, DIFCA and the Registrar,

GDPR	DIFC Law 2020	DIFC Law 2007
General Exemptions (cont'd)		
		including any delegated powers and functions insofar as such powers and functions are designed for protecting members of the public against: (a) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other banking and financial activities and services, including insurance and reinsurance services, financial markets and financial and monetary brokerage services; or (b) dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services.

2. Key definitions

2.1. Personal data

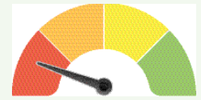
While the core concepts of personal data are similar between the DIFC Law 2020 and the DIFC Law 2007, there are nuanced differences in their definitions of matters such as special categories of data and online identifiers.

The DIFC Law 2020 has moved definitions under DIFC legislation into closer alignment with the GDPR, and particularly by explicitly including online identifiers within the concept of personal data.

GDPR	DIFC Law 2020	DIFC Law 2007
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.	Schedule 1.3: 'personal data' means any information referring to an identified or identifiable natural person. Schedule 1.3: 'identifiable natural person' means a natural living person 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 (1) or more factors specific to his biological, physical, biometric, physiological, mental, genetic, economic, cultural or social identity (and 'Identified Natural Person' is interpreted accordingly).	Schedule 1.3: personal data: any data referring to an identifiable natural person. Schedule 1.3: data: any information which: (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should be processed by means of such equipment; or (c) is recorded as part of a Relevant Filing System or with the intention that it should form part of a Relevant Filing System. Schedule 1.3: identifiable natural person: is a natural living person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his biological, physical, biometric, physiological, mental, economic, cultural or social identity.
Special Categories of Data		
Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	Schedule 1.3: personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person.	Schedule 1.3: personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life.

GDPR	DIFC Law 2020	DIFC Law 2007
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.	Although the concept of 'online identifier' is not itself defined, the DIFC Law 2020 refers to online identifiers within its definition of 'identifiable natural person', see above.	The DIFC Law 2007 does not refer to online identifiers.
Other		
Article 4(6): 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.	Schedule 1.3: 'filing system' means any structured set of personal data that is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographic basis.	Schedule 1.3: relevant filing system: any set of information relating to an identifiable natural person to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

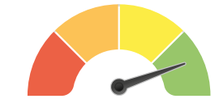
2.2. Pseudonymization



Unlike the DIFC Law 2007, the DIFC Law 2020 makes explicit reference to both anonymisation and pseudonymisation. However, it does not define these concepts in the same explicit manner as the GDPR.

GDPR	DIFC Law 2020	DIFC Law 2007
Anonymization		
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.	Although the DIFC Law 2020 does not explicitly define anonymised or pseudonymised data, it refers to both in Article 22. Specifically, Article 22 provides that where processing must cease personal data should be deleted, anonymised, pseudonymised, or securely encrypted, among other measures.	The DIFC Law 2007 does not define or directly refer to anonymisation.
Pseudonymization		
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.	Although the DIFC Law 2020 does not explicitly define anonymised or pseudonymised data, it refers to both in Article 22. Specifically, Article 22 provides that where processing must cease personal data should be deleted, anonymised, pseudonymised, or securely encrypted, among other measures.	The DIFC Law 2007 does not define or refer to pseudonymisation.

2.3. Controllers and processors



With the introduction of Data Protection Impact Assessment ('DPIA') and data protection officer ('DPO') appointment requirements, the DIFC Law 2020 has moved DIFC legislation into much closer alignment with the GDPR than the DIFC Law 2007. Furthermore, the DIFC Law 2020 contains significantly more extensive obligations and clarifications regarding data processor, subprocessor, and joint controller contracts and agreements than the DIFC Law 2007.

GDPR	DIFC Law 2020	DIFC Law 2007
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.	Schedule 1.3: 'controller' means any person who alone or jointly with others determines the purposes and means of the processing of personal data.	Schedule 1.3: data controller: any person in the DIFC who alone or jointly with others determines the purposes and means of the processing of personal data.
Data Processor		
Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	Schedule 1.3: 'processor' means any person who processes personal data on behalf of a controller.	Schedule 1.3: 'data processor': any person who processes personal data on behalf of a data controller.
Controller and Processor Contracts		
Article 28(3): Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.	Article 24(1): Where processing is to be carried out on behalf of a controller by a processor, the processing shall be governed by a legally binding written agreement between the controller and the processor. A controller shall only enter into agreements with processors that provide sufficient assurances to implement appropriate technical and organisational measures that ensure the processing meets the requirements of this Law and protects a data subject's rights.	The DIFC Law 2007 does not directly stipulate that contracts or agreements are required. Article 16(3): The data controller shall, where processing is carried out on its behalf, choose a data processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and shall ensure compliance with those measures.

GDPR	DIFC Law 2020	DIFC Law 2007
Controller and Processor Contracts (cont'd)		
[Article 28 goes on to stipulate necessary information to be included in such a contract.]	[Article 24 goes on to stipulate necessary information to be included in such a contract.] Article 23(2): Joint controllers shall, by way of legally binding written agreement, define their respective responsibilities for ensuring compliance with the obligations under this Law. Such agreement shall clarify the process for ensuring that a data subject can exercise his rights under this Law and for providing a data subject with the information referred to in Articles 29 and 30.	
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 20 sets out requirements for DPIAs (see section 4.3. for further information).	The DIFC Law 2007 does not address DPIAs.
Data Protection Officer (DPO)		
DPO is not specifically defined, however Article 37 sets out requirements related to DPOs (see section 5.4. below for further information).	Schedule 1.3: 'DPO' means a data protection officer appointed by a controller (including a joint controller), or processor to independently oversee relevant data protection operations in the manner set out in Articles 16, 17, 18 and 19.	The DIFC Law 2007 does not provide requirements for DPOs.

2.4. Children

Consistency with the DIFC Law 2020: Inconsistent

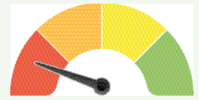
Consistency with the DIFC Law 2007: Inconsistent

In similarity with the DIFC Law 2007, but unlike the GDPR, the DIFC Law 2020 does not generally refer to children's data or provide specific requirements for collecting personal data from children. Article 38(4) of the DIFC Law 2020, though, briefly refers to minors in the context of the non-applicability of exemptions related to the right to object to automated decision-making.

GDPR	DIFC Law 2020	DIFC Law 2007
Children 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 DIFC Law 2020 does not explicitly address children's data..	The DIFC Law 2007 does not 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 DIFC Law 2020 does not explicitly address children's data.	The DIFC Law 2007 does not address children's data.
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.	The DIFC Law 2020 does not explicitly address children's data.	The DIFC Law 2007 does not address children's data.

2.5. Research

Consistency with the DIFC Law 2020: Fairly Inconsistent



Consistency with the DIFC Law 2007: Inconsistent

The DIFC Law 2020 does not address processing for research purposes to the same extent as the GDPR. However, and unlike the DIFC Law 2007, the DIFC Law 2020 provides a general exemption from certain requirements related to the cessation of processing where processing is conducted for research purposes.

GDPR	DIFC Law 2020	DIFC Law 2007
Scientific/Historial Research Definition		
Recital 159: Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. Recital 160: Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.	The DIFC Law 2020 does not explicitly define scientific or historical research.	The DIFC Law 2007 does not address processing for scientific or historical research purposes.
Compatability 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').	Although the DIFC Law 2020 does not explicitly address this matter, Article 22(4) provides that: Notwithstanding Article 22(1), a controller and any relevant processor is not required to securely and permanently delete, anonymise, pseudonymise or encrypt personal data or put it beyond further use, where such personal data: [...] (b) is being used in scientific research activity conducted in the public interest or in the interests of the DIFC in accordance with all applicable laws, in a manner that does not present risks to the rights of data subjects.	The DIFC Law 2007 does not address processing for scientific or historical research purposes.

GDPR	DIFC Law 2020	DIFC Law 2007
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.	Although the DIFC Law 2020 does not explicitly address this matter, Article 22(4) provides that: Notwithstanding Article 22(1), a controller and any relevant processor is not required to securely and permanently delete, anonymise, pseudonymise or encrypt personal data or put it beyond further use, where such personal data: [...] (b) is being used in scientific research activity conducted in the public interest or in the interests of the DIFC in accordance with all applicable laws, in a manner that does not present risks to the rights of data subjects.	The DIFC Law 2007 does not address 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.	Although the DIFC Law 2020 does not explicitly address this matter, Article 22(4) provides that: Notwithstanding Article 22(1), a controller and any relevant processor is not required to securely and permanently delete, anonymise, pseudonymise or encrypt personal data or put it beyond further use, where such personal data: [...] (b) is being used in scientific research activity conducted in the public interest or in the interests of the DIFC in accordance with all applicable laws, in a manner that does not present risks to the rights of data subjects.	The DIFC Law 2007 does not address processing for scientific or historical research purposes.

3. Legal basis

The DIFC Law 2020, the DIFC Law 2007, and the GDPR all provide similar essential legal grounds for processing personal data and additional grounds for processing special categories of data. However, the DIFC Law 2020 is more detailed than either the DIFC Law 2007 or the GDPR in regard to conditions for consent.

GDPR	DIFC Law 2020	DIFC Law 2007
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 10: Any one or more of the following shall constitute a lawful basis for processing personal data: (a) a data subject has given consent, which complies with Article 12, to the processing of that personal data for specific purposes; (b) processing is necessary for the performance of a contract to which a data subject is a party, or in order to take steps at the request of a data subject prior to entering into such contract; (c) processing is necessary for compliance with applicable law that a controller is subject to; (d) processing is necessary in order to protect the vital interests of a data subject or of another natural person; (e) processing is necessary for: (i) performance of a task carried out by a DIFC body in the interests of the DIFC; (ii) exercise of a DIFC body's powers and functions; or (iii) the exercise of powers or functions vested by a DIFC body in a third party to whom personal data is disclosed by the DIFC body; or (f) processing is necessary for the purpose of legitimate interests pursued by a controller or a third party to whom the personal data has been made available, subject to Article 13, except where such interests are overridden by the interests or rights of a data subject.	Article 9: Personal data may only be processed if: (a) the data subject has given his written consent to the processing of that personal data; (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 any legal obligation to which the data controller is subject; (d) processing is necessary for the performance of a task carried out in the interests of the DIFC, or in the exercise of the DIFCA, the DFSA, the Court and the Registrar's functions or powers vested in the data controller or in a third party to whom the personal data are disclosed; or (e) processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party or parties to whom the personal data is disclosed, except where such interests are overridden by compelling legitimate interests of the data subject relating to the data subject's particular situation.

GDPR	DIFC Law 2020	DIFC Law 2007
Sensitive Data (Legal Basis)		
There are specific requirements for processing special categories of data, see Article 9 of the GDPR for further information.	There are specific requirements for processing special categories of data, see Article 11 of the DIFC Law 2020 for further information.	There are specific requirements for processing sensitive data, see Article 10 of the DIFC Law 2007 for further information.
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 12: (1) Consent must be freely given by a clear affirmative act that shows an unambiguous indication of consent if it is to be relied on as a basis for processing under Article 10(1)(a) or under Article 11(1)(a). If the performance of an act by a controller, a data subject or any other party, (including the performance of contractual obligations), is conditional on the provision of consent to process personal data, then such consent will not be considered to be freely given with respect to any processing that is not reasonably necessary for the performance of such act or where the consent relates to excessive categories of personal data. (2) Where processing is based on consent, a controller must be able to demonstrate that consent has been freely given. (3) If the processing is intended to cover multiple purposes, consent must be obtained for each purpose in a manner that is clearly distinguishable, in an intelligible and easily accessible form, using clear and plain language. (4) If a controller seeks to obtain consent for one or more other matters not expressly concerned with the processing of personal data, the request for consent for the processing of personal data must be clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.	The DIFC Law 2007 does not address conditions for consent beyond requiring that consent be 'written' (see Article 9 of the DIFC Law, above).

GDPR	DIFC Law 2020	DIFC Law 2007
Conditions for Consent (cont'd)		
	(5) A data subject may withdraw consent at any time in accordance with the right afforded to data subjects under Article 32. A data subject must be informed of this right and how to exercise it as set out in Article 40 at the time consent is obtained. Withdrawing consent should not require undue effort on the part of the data subject and should be at least as easy as the process of giving consent. Withdrawal of consent does not affect the lawfulness of processing carried out before the date of withdrawal. Where consent is withdrawn a controller must comply with Article 32(3). (6) Other than for the purpose of a Single Discrete Incident, where a controller relies on a data subject's consent for processing, the controller should implement appropriate and proportionate measures to assess the ongoing validity of the consent. This includes considering whether the data subject, acting reasonably, would expect processing to continue based on the consent given, taking into account the circumstances and the terms of such consent. (7) Where such ongoing assessment conducted in accordance with Article 12(6) concludes that a data subject would no longer reasonably expect the processing to be continuing, he must be contacted without delay and asked to re-affirm consent. (8) In the circumstances referred to in Article 12(7), consent shall be deemed to be withdrawn if there is no positive act of re-affirmation of consent within a reasonable period after a data subject has been contacted.	

GDPR	DIFC Law 2020	DIFC Law 2007
Conditions for Consent (cont'd)		
	(9) A controller must be able to demonstrate to the Commissioner that appropriate methods and procedures are in place to manage the recording of consent and the withdrawal of consent, and that periodic evaluations of the same are conducted. (10) Where processing is not a Single Discrete Incident and continues on the basis of consent, a data subject should be given the opportunity to re-affirm or withdraw consent on a periodic basis. (11) A 'Single Discrete Incident' means a processing operation or a collection of processing operations that relate to a: (a) single, non-recurring transaction; or (b) non-recurring and clearly defined purpose that a data subject is seeking to achieve, in each case, with a definable end point. (12) For the avoidance of doubt, consent given for processing to perform a Single Discrete Incident remains subject to all foregoing provisions of this Article except for Article 12(6) and Article 12(10).	
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 DIFC Law 2020 does not explicitly address processing for journalistic or artistic purposes.	The DIFC Law 2007 does not address processing for journalistic or artistic purposes.

4. Controller and processor obligations

Consistency with the DIFC Law 2020: Fairly Consistent

Consistency with the DIFC Law 2007: Fairly Inconsistent

4.1. Data transfers

The DIFC Law 2020 introduces several data transfer mechanisms that are similar to those found in the GDPR, such as Binding Corporate Rules ('BCRs'). In addition, like the DIFC Law 2007, the DIFC Law 2020 continues to include additional mechanisms, such as legitimate interests as recognised in financial markets.

GDPR	DIFC Law 2020	DIFC Law 2007
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 26(1): Processing of personal data that involves the transfer of personal data from the DIFC to a third country or to an international organisation may take place only if: (a) an adequate level of protection for that personal data is ensured by applicable law, as set out in Articles 26(2) and (3), including with respect to onward transfers of personal data; or (b) it takes place in accordance with Article 27. [Note: Article 26 of the DIFC Law 2020 further defines the process of ascertaining adequate protection. In addition, a whitelist of adequate jurisdictions is included in Appendix 3 of the Regulations 2020.]	Article 11: (1) A transfer of personal data to a recipient located in a jurisdiction outside the DIFC may take place only if: (a) an adequate level of protection for that personal data is ensured by laws and regulations that are applicable to the recipient, as set out in Article 11(2); or (b) in accordance with Article 12. (2) For the purposes of Article 11(1), a jurisdiction has an adequate level of protection for that personal data if that jurisdiction is listed as an acceptable jurisdiction under the Regulations or any other jurisdiction as approved by the Commissioner of Data Protection. [Note: A list of 'acceptable jurisdictions' is provided in the DPR 2018.]

GDPR	DIFC Law 2020	DIFC Law 2007

Other Mechanisms for Data Transfers

Article 46(1): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.
(2) The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:
(a) a legally binding and enforceable instrument between public authorities or bodies;
(b) binding corporate rules in accordance with Article 47;
(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2); (e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

Article 27: A transfer or a set of transfers of personal data to a third country or an international organisation may take place on condition that:
(a) the controller or processor in question has provided appropriate safeguards (as described in Article 27(2)), and on condition that enforceable data subject rights and effective legal remedies for data subjects are available;
(b) one of the specific derogations in Article 27(3) applies; or
(c) the limited circumstances in Article 27(4) apply.
(2) The appropriate safeguards referred to in Article 27(1)(a) may be provided for by:
(a) a legally binding instrument between public authorities;
(b) BCRs, subject to Article 27(6);
(c) standard data protection clauses as adopted by the Commissioner in accordance with regulations setting out a procedure for developing such clauses;
(d) an approved code of conduct pursuant to Article 48 together with binding and enforceable commitments of the controller or processor in the third country or the international organisation to apply the appropriate safeguards, including regarding a data subject's rights; or
(e) an approved certification mechanism pursuant to Article 50 together with binding and enforceable commitments of the controller or processor in the third country or the international organisation to apply the appropriate safeguards, including regarding data subjects' rights.
(3) The derogations referred to in Article 27(1)(b) are:
(a) a data subject has explicitly consented to a proposed transfer, after being informed of possible risks of such transfer due to the absence of an adequacy decision or appropriate safeguards;

Article 12: (1) A transfer or a set of transfers of personal data to a recipient which is not subject to laws and regulations which ensure an adequate level of protection within the meaning of Article 11 may take place on condition that:
(a) the Commissioner of Data Protection has granted a permit or written authorisation for the transfer or the set of transfers and the data controller applies adequate safeguards with respect to the protection of this personal data;
(b) the data subject has given his written consent to the proposed transfer;
(c) the transfer is necessary for the performance of a contract between the data subject and the data controller or the implementation of precontractual measures taken in response to the data subject's request;
(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party;
(e) the transfer is necessary or legally required on grounds important in the interests of the DIFC, or for the establishment, exercise or defence of legal claims;
(f) the transfer is necessary in order to protect the vital interests of the data;
(g) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case;

GDPR	DIFC Law 2020	DIFC Law 2007

Other Mechanisms for Data Transfers (cont'd)

(b) the transfer is necessary for the performance of a contract between a data subject and controller or the implementation of pre-contractual measures taken in response to the data subject's request;
(c) the transfer is necessary for the conclusion or performance of a contract that is in the interest of a data subject between a controller and a third party;
(d) the transfer is necessary for reasons of substantial public interest;
(e) the transfer is necessary or legally required in the interests of the DIFC, including in the interests of the DIFC bodies relating to the proper discharge of their functions;
(f) the transfer is necessary for the establishment, exercise or defence of a legal claim;
(g) the transfer is necessary in order to protect the vital interests of a data subject or of other persons where a data subject is physically or legally incapable of giving consent;
(h) the transfer is made in compliance with applicable law and data minimisation principles, set out in Article 9(1)(e), from a register that is:
(i) intended to provide information to the public; and
(ii) open for viewing either by the public in general or by any person who can demonstrate a legitimate interest;
(i) subject to Article 28, the transfer is:
(i) necessary for compliance with any obligation under Applicable Law to which the controller is subject; or (ii) made at the reasonable request of a regulator, police or other government agency or competent authority;

(h) the transfer is necessary for compliance with any legal obligation to which the data controller is subject or the transfer is made at the request of a regulator, police or other government agency;

(i) the transfer is necessary to uphold the legitimate interests of the data controller recognised in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by legitimate interests of the data subject relating to the data subject's particular situation; or

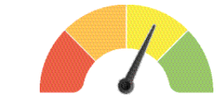
(j) the transfer is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering or counter terrorist financing obligations or the prevention or detection of any crime that apply to a data controller.

(2) The Court has jurisdiction to hear and determine any appeal in relation to a decision of the Commissioner of Data Protection to refuse to issue a permit referred to in Article 12(1)(a) and his decision is final and binding upon the data controller.

GDPR	DIFC Law 2020	DIFC Law 2007
Other Mechanisms for Data Transfers (cont'd)		
(j) subject to international financial standards, the transfer is necessary to uphold the legitimate interests of a controller recognised in international financial markets, except where such interests are overridden by the legitimate interests of the data subject relating to the data subject's particular situation; or (k) the transfer is necessary to comply with applicable anti-money laundering or counterterrorist financing obligations that apply to a controller or processor or for the prevention or detection of a crime. (4) Where a transfer could not be based on one of the provisions in this Article 27(1) to (3) or Article 26, such transfer to a third country or an international organisation may take place only if: (a) the transfer is not repeating or part of a repetitive course of transfers; (b) concerns only a limited number of data subjects; (c) is necessary for the purposes of compelling legitimate interests pursued by the controller that are not overridden by the interests or rights of the data subject; and (d) the controller has completed a documentary assessment of all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. (5) A controller shall inform the Commissioner of any transfer made pursuant to Article 27(4) and shall, in addition to providing the information referred to in Articles 29 or 30, as applicable, inform the data subject of the transfer and the compelling legitimate interests. (6) A public authority subject to DIFC law may not rely on Articles 27(3)(a), (b) and (c), or on Article 27(4).		

GDPR	DIFC Law 2020	DIFC Law 2007
Other Mechanisms for Data Transfers (cont'd)		
	[Note: Article 27(7) to (11) clarifies the processes for BCRs.]	
Data Localisation		
Not applicable.	The DIFC Law 2020 does not explicitly provide data localisation requirements	The DIFC Law 2007 does not explicitly provide data localisation requirements.

4.2. Data processing records



Consistency with the DIFC Law 2020: Fairly consistent

Consistency with the DIFC Law 2007: Fairly Inconsistent

The DIFC Law 2020 and the GDPR require both data controllers and data processors to maintain data processing records, whereas the DIFC Law 2007 only explicitly outlines obligations for data controllers. Unlike the GDPR, however, the DIFC Law 2020 also establishes registration (or data processing notification) requirements.

GDPR	DIFC Law 2020	DIFC Law 2007
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 15: (1) A controller shall maintain a written record, which may be in electronic form, of processing activities under its responsibility, which shall contain at least the following information: (a) name and contact details of the controller, its appointed DPO, where applicable, and joint controller, if any; (b) the purpose(s) of the processing; (c) a description of the categories of data subjects; (d) a description of the categories of personal data; (e) categories of recipients to whom the personal data has been or will be disclosed, including recipients in third countries and international organisations; (f) where applicable, the identification of the third country or international organisation that the personal data has or will be transferred to and, in the case of transfers under Article 27, the documentation of suitable safeguards; (g) where possible, the time limits for erasure of the different categories of personal data; and (h) where possible, a general description of the technical and organisational security measures referred to in Article 14(2). [...] (3) The DIFCA Board of Directors may make regulations on the procedures relating to recording of processing activities under this Article 15. The Regulations 2020, Section 2.1: For the purposes of Article 15(1) of the Law,	Article 19(1): A data controller shall establish and maintain records of any personal data processing operations or set of such operations intended to secure a single purpose or several related purposes. [Note: The DPR 2018 clarifies in Article 6.1.1: A data controller must record the following information in relation to its personal data processing operations: (a) description of the personal data processing being carried out; (b) an explanation of the purpose for the personal data processing; (c) the data subjects or class of data subjects whose personal data is being processed; (d) a description of the class of personal data being processed; and (e) a list of the jurisdictions to which personal data may be transferred by the data controller, along with an indication as to whether the particular jurisdiction has been assessed as having adequate levels of protection for the purposes of Articles 11 and 12 of the Law.]	

GDPR	DIFC Law 2020	DIFC Law 2007
Data Controller Obligation (cont'd)		
	a controller must record at least the following information in relation to its personal data processing operations: (a) description of the personal data processing being carried out; (b) an explanation of the purpose for the personal data processing; (c) the data subjects or class of data subjects whose personal data is being processed; (d) a description of the class of personal data being processed; and (e) a list of the jurisdictions to which personal data may be transferred by the controller, along with an indication as to whether the particular jurisdiction has been assessed as having adequate levels of protection for the purposes of Articles 26 and 27 of the Law.	
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 DPO; (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	Article 15(2): A processor shall maintain a written record of all categories of processing activities carried out on behalf of a controller containing the information specified in Article 15(1).	The DIFC Law 2007 does not specify obligations for data processors to maintain data processing records.

GDPR	DIFC Law 2020	DIFC Law 2007

Data Processor Obligation (cont'd)

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).		

Records Format

Article 30(3): The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.	Article 15(1): A controller shall maintain a written record, which may be in electronic form, of processing activities under its responsibility [...]	Neither the DIFC Law 2007 nor the DPR 2018 address the format for data processing records.

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 52(1): The Commissioner may require a controller or processor by written notice to: [...] (b) produce the processing records, or copies thereof, required to be maintained under Article 15.	Although neither the DIFC Law 2007 nor the DPR 2018 explicitly refer to making data processing records available, there are provisions for notifying the Commissioner of Data Protection in certain circumstances, such as when processing sensitive data or for data transfers to jurisdictions that have not been deemed as providing adequate protection. Article 6.3.2 of the DPR 2018 further clarifies that the information to be contained in such notification is the same type of information as that which is to be maintained in a data processing record. In addition, Article 27 of the DIFC Law 2007 provides: (1) The Commissioner of Data Protection may require a data controller by written notice to: (a) give specified information; or (b) produce specified documents which relate to the processing of personal data.

GDPR	DIFC Law 2020	DIFC Law 2007

Exemptions

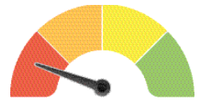
Article 30(5): The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the 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 DIFC Law 2020 does not establish specific exemptions from record-keeping requirements.	The DIFC Law 2007 does not provide specific exemptions from data processing record requirements.

General Data Processing Notification

Not applicable.	Article 14: (7) A controller or processor shall register with the Commissioner by filing a notification of processing operations, which shall be kept up to date through amended notifications. (8) Notifications referred to in Article 14(7) shall be: (a) kept on a publicly available register maintained by the Commissioner; and (b) accompanied by such fee as may be prescribed in regulations made by the DIFCA Board of Directors. [Note: Section 3 of the Regulations 2020 provides further obligations regarding data processing notification/ registration. See Dubai International Financial Centre – Data Processing Notification for further information.	While there is no general data processing notification ('DPN') requirement, Article 6.3.1 of the DPR 2018 stipulates: For the purposes of Articles 19(4)(b) and 19(4)(c) of the Law, a data controller must notify the Commissioner of Data Protection of the following personal data processing operations or set of such operations: (a) any personal data processing operation or set of operations involving the processing of sensitive personal data; and (b) any personal data processing operation or set of operations involving the transfer of personal data to a recipient outside of the DIFC which is not subject to laws and Regulations which ensure an adequate level of protection.

4.3. Data protection impact assessment

Consistency with the DIFC Law 2020: Fairly Consistent



Consistency with the DIFC Law 2007: Inconsistent

Unlike the DIFC Law 2007, the DIFC Law 2020 establishes DPIA requirements.

Furthermore, the DPIA requirements under the DIFC Law 2020 are very similar, although slightly more detailed, than those under the GDPR. For instance, the DIFC Law 2020 addresses joint controller and processor obligations related to DPIAs more extensively..

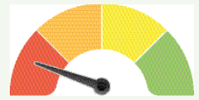
GDPR	DIFC Law 2020	DIFC Law 2007
When is a DPIA Required		
Article 35(1): Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, 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 20: (1) Prior to undertaking high risk processing activities a controller shall carry out an assessment of the impact of the proposed processing operations on the protection of personal data, considering the risks to the rights of the data subjects concerned. A controller may also elect to carry out such assessment in relation to the processing of personal data that is not a high risk processing activity. [...] (4) The Commissioner may at his discretion publish a non-exhaustive list of types or categories of processing operations that are considered to be high risk processing activities. Such a list is not intended to be exhaustive and does not absolve a controller from responsibility for complying with this Law in all respects with regard to high-risk processing activities. (5) The Commissioner may also publish a list of the types or categories of processing operations for which no DPIA. Schedule 1.3: 'High risk processing activities' means processing of personal data where one (1) or more of the following applies: (a) processing that includes the adoption of new or different technologies or methods, which creates a materially increased risk to the security or rights of a data subject or renders it more difficult for a data subject to exercise his rights;	The DIFC Law 2007 does not provide requirements for DPIAs.

GDPR	DIFC Law 2020	DIFC Law 2007
When is a DPIA Required (cont'd)		
	(b) a considerable amount of personal data will be processed (including staff and contractor personal data) and where such processing is likely to result in a high risk to the data subject, including due to the sensitivity of the personal data or risks relating to the security, integrity or privacy of the personal data; (c) the processing will involve a systematic and extensive evaluation of personal aspects relating to natural persons, 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; or (d) a material amount of special categories of personal data is to be processed.	
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.	Article 20(6): A DPIA shall contain at least: (a) a systematic description of the foreseen processing operations and the purpose(s) of the processing, including, where applicable, the legitimate interest pursued by a controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purpose(s); (c) identification and consideration of the lawful basis for the processing, including: (i) where legitimate interests are the basis for processing, an analysis and explanation of why a controller believes the interests or rights of a data subject do not override its interests; and (ii) where consent is the basis for processing, validation that such consent is validly obtained, consideration of the impact of the withdrawal of consent to such processing and of how a controller will ensure compliance with the exercise of a data subject's right to withdraw consent;	The DIFC Law 2007 does not provide requirements for DPIAs.

GDPR	DIFC Law 2020	DIFC Law 2007
DPIA Content Requirements (cont'd)		
	(d) an assessment of the risks to the rights of data subjects; and (e) 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 Law, taking into account the rights and legitimate interests of data subjects and other concerned persons.	
Consultation with Authority		
Article 36(1): The controller shall consult the supervisory authority prior to processing where a DPIA 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].	Article 21(1): A controller shall consult the Commissioner where a DPIA under Article 20 indicates that, despite taking the measures referred to in Article 20(6)(e), the risks to the rights of data subjects remain particularly high and the controller has already carried out or wishes to commence or continue carrying out a processing activity. [Article 21 goes on to detail requirements related to such prior consultation].	The DIFC Law 2007 does not provide requirements for DPIAs.

4.4. Data protection officer appointment

Consistency with the DIFC Law 2020: Fairly consistent



Consistency with the DIFC Law 2007: Inconsistent

Unlike the DIFC Law 2007, the DIFC Law 2020 establishes extensive DPO requirements.

There are several similarities between the GDPR and the DIFC Law 2020 in regard to DPO requirements, although the DIFC Law 2020 details additional obligations such as on the location of the DPO and provisions for annual assessments to be conducted by the DPO. See Dubai International Finance Centre - Data Protection Officer Appointment for further information.

GDPR	DIFC Law 2020	DIFC Law 2007
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.	Article 18: (1) A controller or processor shall ensure that: (a) its DPO is properly involved in a timely manner, on all issues relating to the protection of personal data and is given sufficient resources necessary to carry out the role; (b) its DPO is free to act independently; and (c) any additional tasks and duties fulfilled by its DPO, other than those required under this Law, do not result in a conflict of interest or otherwise prevent the proper performance of the role of the DPO. (2) A data subject may contact the DPO of a controller or processor with regard to all issues related to processing of his personal data and to the exercise of his rights under this Law. (3) A DPO shall perform at least the following tasks: (a) monitor a controller or processor's compliance with: (i) this Law; (ii) any other data protection or privacy-related laws or regulations to which the organisation is subject within the DIFC; and (iii) any policies relating 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;	The DIFC Law 2007 does not provide requirements for DPOs.

GDPR	DIFC Law 2020	DIFC Law 2007

DPO Tasks (cont'd)

	(b) inform and advise a controller or processor and its employees who carry out processing of its obligations pursuant to this Law and to other data protection provisions, including where the organisation is subject to overseas provisions with extra-territorial effect; (c) provide advice where requested in relation to DPIAs undertaken pursuant to Article 20; (d) cooperate with the Commissioner in accordance with Article 17(3); (e) act as the contact point for the Commissioner on issues relating to processing; and (f) receive and act upon any relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions issued or made by the Commissioner.	
	Article 19: (1) Where a controller is required to appoint a DPO under Articles 16(2) or 16(3), the DPO shall undertake an assessment of the controller's processing activities, at least once per year ('the Annual Assessment'), which shall be submitted to the Commissioner. (2) A controller shall report on its processing activities in the Annual Assessment and indicate whether it intends to perform high risk processing activities in the following annual period. (3) The Commissioner shall prescribe and make publically available the format, required content and deadline for submission of Annual Assessments.	The DIFC Law 2007 does not provide requirements for DPOs.

GDPR	DIFC Law 2020	DIFC Law 2007

When is a DPO Required

Article 37(1): The controller and the processor shall designate a DPO 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 16: (1) A controller or processor may elect to appoint a DPO that meets the requirements of Article 17. (2) Notwithstanding Article 16(1), a DPO shall be appointed by: (a) DIFC Bodies, other than the Courts acting in their judicial capacity; and (b) a controller or processor performing high risk processing activities on a systematic or regular basis. (3) A controller or processor to which Article 16(2)(b) does not apply may be required to designate a DPO by the Commissioner. (4) If a controller or processor is not required to appoint a DPO, it shall clearly allocate responsibility for oversight and compliance with respect to data protection duties and obligations under this Law, or any other applicable data protection law, within its organisation and be able to provide details of the persons with such responsibility to the Commissioner upon request.	The DIFC Law 2007 does not provide requirements for DPOs.

Group Appointments

Article 37(2): A group of undertakings may appoint a single DPO provided that a DPO is easily accessible from each establishment.	Article 16: (5) The role of a DPO may be performed by a member of a controller's or processor's staff, an individual employed within a controller's or processor's Group in accordance with Article 16(6) or by a third party under a service contract. (6) A Group may appoint a single DPO provided that he is easily accessible from each entity in the Group.	The DIFC Law 2007 does not provide requirements for DPOs.

Notification of DPO

Article 37(7): The controller or the processor shall publish the contact details of the DPO and communicate them to the supervisory authority.	Article 16(8): A controller or processor shall publish the contact details of its DPO in a manner that is readily accessible to third parties, such that a third party could determine how to contact the DPO without disproportionate effort. On request, a controller or processor shall confirm the identity of its DPO to the Commissioner in writing.	The DIFC Law 2007 does not provide requirements for DPOs.

GDPR	DIFC Law 2020	DIFC Law 2007
Qualifications		
Article 37(5): The DPO 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.	Article 16(7): A DPO must reside in the UAE unless he is an individual employed within the organisation's Group and performs a similar function for the Group on an international basis. Article 17: (1) A DPO must have knowledge of this Law and its requirements and shall ensure a controller or processor monitors compliance with this Law. (2) A DPO must: (a) have the ability to fulfil the tasks in Article 18; (b) be able to perform his duties and tasks in an independent manner, and be able to act on his own authority; (c) have direct access and report to senior management of the controller or processor; (d) have sufficient resources to perform his duties in an effective, objective and independent manner; and (e) have timely and unrestricted access to information within the controller or processor organisation to carry out his duties and responsibilities under this Law. (3) Without prejudice to the mandatory notification requirements under this Law, a DPO shall be transparent and cooperative with the Commissioner and shall notify the Commissioner of all relevant information within the controller or processor organisation, other than information that is subject to legal privilege or a conflicting obligation of non-disclosure under applicable law. (4) Subject to Article 18(1)(c), a DPO may hold other roles or titles within a controller or processor or within each such Group, and may fulfil additional tasks and duties other than those described in this Law.	The DIFC Law 2007 does not provide requirements for DPOs.

4.5. Data security and data breaches

Consistency with the DIFC Law 2020: Fairly consistent

Consistency with the DIFC Law 2007: Fairly inconsistent

The DIFC Law 2020 introduces significantly more detailed data security requirements than the DIFC Law 2007, including obligations for data breach notifications to data subjects. While there are several similarities between the DIFC Law 2020 and the GDPR, the DIFC Law 2020 does not clarify exceptions from breach notification requirements, is less clear in its definitions of security measures, and does not specify an exact timeframe for breach notifications. See Dubai International Financial Centre - Data Breach for further information.

GDPR	DIFC Law 2020	DIFC Law 2007
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 14: (2) A controller or processor is required to implement appropriate technical and organisational measures to demonstrate that processing is performed in accordance with this Law, including: (a) taking into account: (i) the nature, scope, context and purpose of the processing; (ii) the risks presented by the processing to a relevant data subject; and (iii) prevailing information security good industry practice. (b) ensuring a level of security: (i) appropriate to the risks associated with processing, taking account of any wilful, negligent, accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of or access to personal data; and (ii) against all other unlawful forms of processing; (c) ensuring that, by default, only personal data necessary for each specific purpose is processed. This obligation applies to the amount and type of personal data collected, the extent of the processing, the period of storage and accessibility; and (d) reviewing and updating such measures where necessary to reflect legal, operational and technical developments.	Article 16: The data controller shall implement appropriate technical and organisational measures to protect personal data against wilful, negligent, accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of processing, in particular where the processing of personal data is performed pursuant to Article 10 or Article 12 above. (2) Having regard to the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected.

GDPR	DIFC Law 2020	DIFC Law 2007

Security Measures Defined (cont'd)

(3) a controller or processor shall integrate necessary measures into the processing in order to meet the requirements of this Law, protect a data subject's rights and follow the principle of 'data protection by design and by default', which shall at least require assurances that:
(i) processing is designed to reinforce data protection principles such as data minimisation at the time of determining the means for Processing and at the time of processing itself; and
(ii) by default, only personal data that is necessary for each specific purpose is processed, and that personal data is not made accessible to an indefinite number of persons without the data subject's intervention.

Article 22: (1) Where the basis for processing changes, ceases to exist or a controller is required to cease processing due to the exercise of a data subject's rights, the controller shall ensure that all personal data, including personal data held by processors is:
(a) securely and permanently deleted;
(b) anonymised so that the data is no longer personal data and no data subject can be identified from the data including where the data is lost, damaged or accidentally released;
(c) pseudonymised;
(d) securely encrypted; or
(2) Where a controller is unable to ensure that personal data is securely and permanently deleted, anonymised, pseudonynmised or securely encrypted, the personal data must be archived in a manner that ensures the data is put beyond further use.
(3) 'Put beyond further use' in Article 22(2) means that:

GDPR	DIFC Law 2020	DIFC Law 2007

Security Measures Defined (cont'd)

(a) a controller and a relevant processor are unable to use the personal data to inform any decision with respect of the data subject or in a manner that affects the data subject in any way, other than where such personal data needs to be cross-checked by automated means solely in order to prevent further processing of personal data related to the data subject;
(b) no party has access to the personal data other than the controller and any relevant processor;
(c) personal data is protected by appropriate technical and organisational security measures that are equivalent to those afforded to live personal data; and
(d) a controller and any relevant processor have in place and must comply with a strategy for the permanent deletion, anonymisation, pseudonymisation or secure encryption of the personal data, complies and can demonstrate compliance with such policy.

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 41(1): If there is a personal data breach that compromises a data subject's confidentiality, security or privacy, the controller involved shall, as soon as practicable in the circumstances, notify the personal data breach to the Commissioner.

Article 16(4): In the event of an unauthorised intrusion, either physical, electronic or otherwise, to any personal data database, the data controller or the data processor carrying out the data controller's function at the time of the intrusion, shall inform the Commissioner of Data Protection of the incident as soon as reasonably practicable.

GDPR	DIFC Law 2020	DIFC Law 2007
Timeframe for Breach Notification		
See Article 33(1) above.	See Article 41(1) above.	See Article 16(4) 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 42(1): When a personal data breach is likely to result in a high risk to the security or rights of a data subject, the controller shall communicate the personal data breach to an affected data subject as soon as practicable in the circumstances. If there is an immediate risk of damage to the data subject, the controller shall promptly communicate with the affected data subject.	The DIFC Law 2007 does not provide for breach notifications to data subjects.
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.	Article 41(2): A processor shall notify a relevant controller without undue delay after becoming aware of a personal data breach.	See Article 16(4) above.
Exceptions		
Article 34(3): The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.	Article 41(5): Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases when available. Article 42(3): Where a communication to the individual data subjects referred to in Article 42(1) will involve disproportionate effort, a public communication or similar measure by the controller whereby the data subjects are informed in an equally effective manner shall be sufficient.	There are no specific exemptions from data security or data breach requirements in the DIFC Law 2007.

4.6. Accountability

Consistency with the DIFC Law 2020: Fairly consistent

Consistency with the DIFC Law 2007: Fairly inconsistent

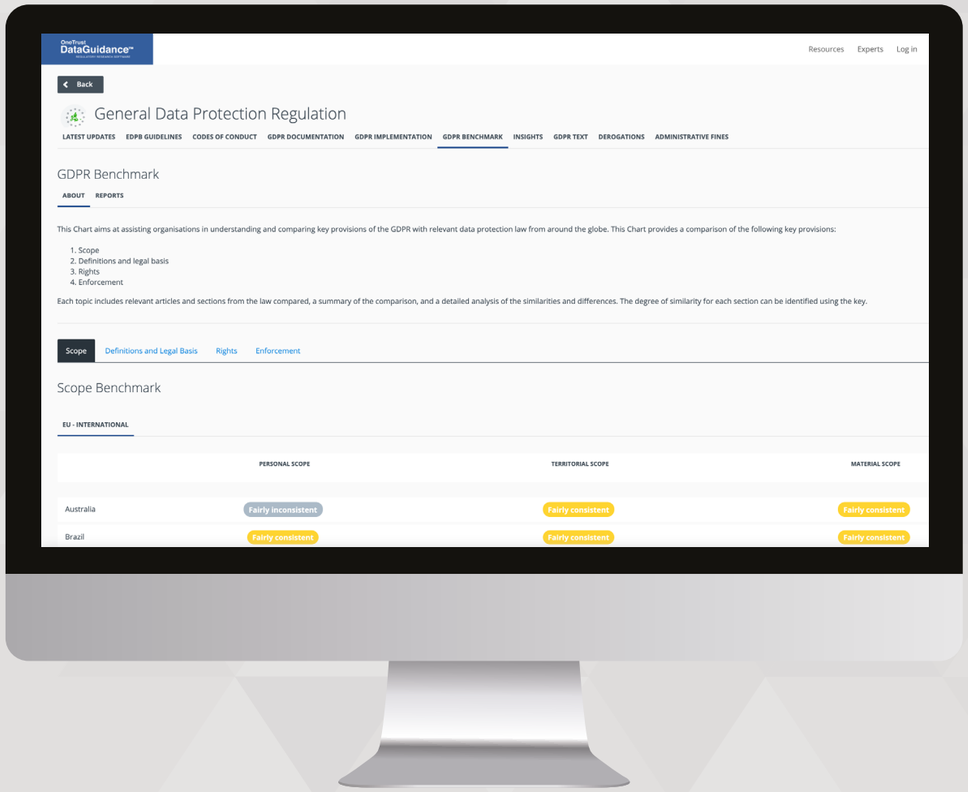
Unlike the DIFC Law 2007, the DIFC Law 2020 explicitly addresses accountability requirements and the liabilities of data processors. While there are similarities with the GDPR, the DIFC Law 2020 introduces more detailed obligations, including requiring that a program is established to demonstrate compliance.

GDPR	DIFC Law 2020	DIFC Law 2007
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.] 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 9(2): A controller or processor shall be responsible for, and must be able to demonstrate to the Commissioner its compliance with, Article 9(1). [Article 9(1) establishes requirements for lawfulness, fairness, and transparency, purpose limitations, compliance with data subject rights, storage limitation, accuracy, and appropriate security measures.] Article 14(1): A controller or processor is required to establish a program to demonstrate compliance with this Law, the level and detail of which will depend on the scale and resources of the controller or the processor, the categories of personal data being processed and the risks to the data subjects.	The DIFC Law 2007 does not directly address a principle of accountability.
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 24: (9) If a processor infringes this Law by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing and will assume all the responsibilities and obligations of a controller. (10) Both a controller and processor are in breach of this Law if they commence mutually agreed processing activity without a written agreement referred to in Articles 24(1) and 24(3).	Article 35: A data controller who: (a) does an act or thing that the data controller is prohibited from doing by or under this Law and the Regulations; (b) does not do an act or thing that the data controller is required or directed to do under this Law and the Regulations; or (c) otherwise contravenes a provision of this Law and the Regulations; commits a contravention of this Law. [Note: the DIFC Law 2007 does not directly address the liability of data processors.]

Global Regulatory Research Software

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

Monitor regulatory developments, mitigate risk, and achieve global compliance



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

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

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

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

- Scope
- Rights
- Definitions and legal basis
- Enforcement

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

OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

Start your free trial at
www.dataguidance.com

GDPR	DIFC Law 2020	DIFC Law 2007
Liability of Data Controllers and Data Processors (cont'd)		
	Article 64: (2) Any controller involved in processing that infringes this Law shall be liable for the damage caused. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Law specifically directed to processors or where it has acted outside or contrary to the lawful instructions of the controller. (3) Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are responsible for any damage caused by processing, each person shall be held jointly and severally liable for the entire damage in order to ensure effective compensation of the data subject.	

5. Rights

5.1. Right to erasure

The DIFC Law 2020 provides for a right to erasure that is more closely aligned to the GDPR than the DIFC Law 2007, particularly in terms of the grounds for erasure, exceptions, timeframes, and fees. While there are nuanced differences between the GDPR and the DIFC Law 2020, the key provisions establishing the right to erasure and the exercise of this right are consistent.

GDPR	DIFC Law 2020	DIFC Law 2007
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 33(2): Subject to Article 33(3), the data subject has the right to require the controller to erase the data subject's personal data where: (a) the processing of the personal data is no longer necessary in relation to the purposes for which it was collected; (b) a data subject has withdrawn consent to the processing where consent was the lawful basis for processing and there is no other lawful basis, provided that in such circumstances the controller must comply with Article 22; (c) the processing is unlawful or the personal data is required to be deleted to comply with applicable law to which the controller is subject; or (d) the data subject objects to the processing and there are no overriding legitimate grounds for the controller to continue with the processing.	Article 17: A data subject has the right to obtain from the data controller upon request, at reasonable intervals and without excessive delay or expense: [...] (c) as appropriate, the rectification, erasure or blocking of personal data the processing of which does not comply with the provisions of the Law.

GDPR	DIFC Law 2020	DIFC Law 2007
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 29(1): Where personal data has not been obtained from the data subject, a controller shall provide the data subject with at least the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language: [...] (h) any necessary information regarding the specific circumstances in which the personal data is processed, to ensure fair and transparent processing in respect of the data subject, including: [...] (ii) notice 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.	Article 13: Data controllers shall provide a data subject whose personal data it collects from the data subject with at least the following information as soon as possible upon commencing to collect personal data in respect of that data subject: [...] (c) any further information in so far as such is necessary, having regard to the specific circumstances in which the personal data are collected, to guarantee fair processing in respect of the data subject, such as: [...] (iii) the existence of the right of access to and the right to rectify the personal data.
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 33(8): 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, providing written confirmation to the data subject reasons for the refusal.	Article 17 provides that the right to erasure should be available without 'excessive delay or expense.'

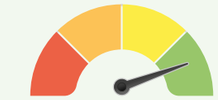
GDPR	DIFC Law 2020	DIFC Law 2007
Response Timeframe		
Article 12(3): The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.	Although the DIFC Law 2020 does not explicitly refer to timeframes in relation to erasure requests, it does specify that access requests should be responded to without charge within one month (see section 6.4. below). In addition, Article 33(7) provides: If a data subject request under Article 33(1) is particularly complex, or requests are numerous, the controller may send notice to the data subject, within one month, to increase the period for compliance by a further two months citing the reasons for the delay.	Article 17 provides that the right to erasure should be available without 'excessive delay or expense.'
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.	Article 33: (11) Where a controller complies with a request under Article 33(1)(b) it shall not disclose the personal data of other individuals in a way that may infringe their rights under applicable law and the controller may redact or otherwise obscure personal data relating to such other individuals. Where the data subject's request is received by electronic means, and unless otherwise requested by the data subject, the information may be provided in a commonly used electronic form. (12) The information to be supplied pursuant to a request under this Article 33 must be supplied by reference to the data in question at the time the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.	The DIFC Law 2007 does not address the format of a response to a request to erase data.

GDPR	DIFC Law 2020	DIFC Law 2007
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.	Article 33: (11) Where a controller complies with a request under Article 33(1)(b) it shall not disclose the personal data of other individuals in a way that may infringe their rights under applicable law and the controller may redact or otherwise obscure personal data relating to such other individuals. Where the data subject's request is received by electronic means, and unless otherwise requested by the data subject, the information may be provided in a commonly used electronic form. (12) The information to be supplied pursuant to a request under this Article 33 must be supplied by reference to the data in question at the time the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.	The DIFC Law 2007 does not address the format of a response to a request to erase data.
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.	Article 33(6): A controller shall direct all recipients and processors to rectify or erase personal data where the respective right is properly exercised or to cease processing and return or erase the personal data where the right to object is validly exercised. In such circumstances, Article 22 applies to the erasure of the personal data by both the controller and the processor.	The DIFC Law 2007 does not address this matter.

GDPR	DIFC Law 2020	DIFC Law 2007
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 33: (3) The controller is only required to comply with a request by a data subject to erase personal data where: (a) one of the conditions in Article 33(2) applies; and (b) subject to Article 33(4), the controller is not required to retain the personal data in compliance with applicable law to which it is subject or for the establishment or defence of legal claims. (4) Where rectification or erasure of personal data is not feasible for technical reasons, then the controller is not in violation of this Law for failing to comply with a request for rectification or erasure of the personal data, in accordance with Articles 33(1)(c), 33(2)(a) or Article 33(2)(d) as applicable, if: (a) the controller collected the personal data from the data subject; and (b) the information provided to the data subject under Article 29(1)(h)(ix) was explicit, clear and prominent with respect to the manner of processing the personal data and expressly stated that rectification or erasure (as the case may be) of the personal data at the request of the data subject would not be feasible. [...] (8) 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, providing written confirmation to the data subject reasons for the refusal. (9) A controller must be able to demonstrate to the Commissioner upon request that a data subject's request made in accordance with Article 33(8) is manifestly unfounded or excessive.	The DIFC Law 2007 does not provide specific exemptions in regard to data subject rights.

GDPR	DIFC Law 2020	DIFC Law 2007
Exceptions (cont'd)		
	(9) A controller must be able to demonstrate to the Commissioner upon request that a data subject's request made in accordance with Article 33(8) is manifestly unfounded or excessive. (10) If a controller has reasonable doubts as to the identity of a data subject asserting a right under this Article 33, it may require the data subject to provide additional information sufficient to confirm the individual's identity. In such cases, the time period for complying with the data subject request does not begin until the controller has received information or evidence sufficient to reasonably identify that the person making the request is the data subject.	

5.2. Right to be informed



Consistency with the DIFC Law 2020: Consistent

Consistency with the DIFC Law 2007: Fairly consistent

The DIFC Law 2020, the DIFC Law 2007, and the GDPR all establish similar provisions for the right to be informed. The DIFC Law 2020, though, is more closely aligned to the GDPR in terms of format and intelligibility requirements, as well as in regard to the variations in information to be provided when personal data is obtained indirectly.

GDPR	DIFC Law 2020	DIFC Law 2007
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,	Article 29(1): A controller shall provide a data subject from whom it collects personal data with at least the following information, in a concise, transparent, intelligible and easily accessible form, using clear and plain language, at the time of collecting the personal data to enable the data subject to assess the implications of providing his personal data: (a) the identity and contact details of the controller; (b) the contact details of the DPO, if applicable; (c) the purposes of the processing, as well as its lawful basis under this Law; (d) if the controller's lawful basis for the processing is legitimate interests or compliance with any applicable law to which the controller is subject, the controller shall state clearly what those legitimate interests or compliance obligations are; (e) the categories of personal data relating to the data subject that are being processed; (f) the recipients or categories of recipients of the personal data; (g) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation, or in the case of transfers referred to in Articles 27(1)(a), 27(2)(b) or 27(3)(b), 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; and	Article 13(1): Data controllers shall provide a data subject whose personal data it collects from the data subject with at least the following information as soon as possible upon commencing to collect personal data in respect of that data subject: (a) the identity of the data controller; (b) the purposes of the processing for which the personal data are intended; (c) any further information in so far as such is necessary, having regard to the specific circumstances in which the personal data are collected, to guarantee fair processing in respect of the data subject, such as: (i) the recipients or categories of recipients of the personal data; (ii) whether replies to questions are obligatory or voluntary, as well as the possible consequences of failure to reply; (iii) the existence of the right of access to and the right to rectify the personal data; (iv) whether the personal data will be used for direct marketing purposes; and (v) whether the personal data will be processed on the basis of Article 12(1)(i) or Article 10(1)(g).

GDPR	DIFC Law 2020	DIFC Law 2007

Informed Prior to/at Collection (cont'd)

GDPR	DIFC Law 2020	DIFC Law 2007
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.	(h) any further information in so far as such is necessary, having regard to the specific circumstances in which the personal data is collected, to ensure fair and transparent processing in respect of the data subject, including: (i) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (ii) 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; (iii) where the processing is based on the data subject's consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (iv) the right to lodge a complaint with the Commissioner; (v) whether the personal data is obtained pursuant to 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 the possible consequences of failure to provide such data; (vi) if applicable, the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the possible outcomes of such processing for the data subject; (vii) whether replies to questions are obligatory or voluntary, as well as the possible consequences of failure to reply; (viii) whether the personal data will be used for direct marketing purposes; and	

GDPR	DIFC Law 2020	DIFC Law 2007

Informed Prior to/at Collection (cont'd)

GDPR	DIFC Law 2020	DIFC Law 2007
	(ix) if the controller intends to process personal data in a manner that will restrict or prevent the data subject from exercising his rights to request rectification or erasure of personal data in accordance with Article 33, or to object to the processing of the personal data in accordance with Article 34. In such cases, the controller shall: 1. include a clear and explicit explanation of the expected impact on such rights; and 2. satisfy itself that the data subject understands and acknowledges the extent of any such restrictions.	

What Information is to be Provided

GDPR	DIFC Law 2020	DIFC Law 2007
See Article 13(1) and (2) above.	See Article 29(1) above.	See Article 13(1) above.

When Data is from Third Party

GDPR	DIFC Law 2020	DIFC Law 2007
In addition to the information required under Article 13, Article 14(2) specifies that where information is not obtained directly from the data subject then the data subject must be provided with information on the legitimate interests pursued by the controller or by a third party where the processing is based on point (f) of Article 6(1). 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.	Article 30 stipulates information to be provided to data subjects when their data is obtained from a third party, with similar variations as that made by Article 14 of the GDPR.	Article 14(1) requires the same information to be provided to data subjects when personal data is not collected directly from the data subject as that set out in Article 13(1), with one exception: the requirement to inform 'whether replies to questions are obligatory or voluntary, as well as the possible consequences of failure to reply' is removed, and a requirement to inform of 'the categories of personal data concerned' is added.

GDPR	DIFC Law 2020	DIFC Law 2007
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.	Both Articles 29 and 30 establish that information should be provided in a 'concise, transparent, intelligible and easily accessible form, using clear and plain language.'	The DIFC Law 2007 does not specify intelligibility requirements in general terms in relation to the right to be informed. However, Article 17(b) provides that a data subject has the right to obtain in response to a request: 'communication to him in an intelligible form of the personal data undergoing processing and of any available information as to its source.'
Format		
See Article 12(1) above.	Article 31: (1) Subject to Article 31(2), the information to be provided under Articles 29 and 30 shall be provided in writing, including, where appropriate, by electronic means. (2) The information to be provided under Articles 29 and 30 may be provided orally upon a data subject's request, including where the personal data is being collected by means of a telephone conversation between the controller and the data subject, on the condition that the identity of the data subject has been verified at the time of the request. (3) A controller may comply with the requirements under Articles 29 and 30, to the extent that the required information is contained within publicly available policies maintained by the controller, by clearly directing the data subject to such policies. Such policies must be written in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The controller may include within such policies links directing the data subject to additional information about the processing.	The DIFC Law 2007 does not address the format of the information to be provided under Articles 13 and 14.

GDPR	DIFC Law 2020	DIFC Law 2007
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.	Article 29(2): Article 29(1) shall not require a controller to provide information the data subject already has. Article 30(3): Article 30(1) shall not apply: (a) to require the controller to provide information the data subject already has; (b) to require the provision of such information if it proves impossible or would involve a disproportionate effort. (c) where disclosure is expressly required by a requesting authority or an applicable law 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 in accordance with applicable law to which the controller is subject, including a statutory obligation of secrecy.	Article 13(2): A data controller need not provide that information otherwise required by Article 13(1) to the data subject if the data controller reasonably expects that the data subject is already aware of that information. Article 14(2): Article 14(1) shall not apply to require: (a) the data controller to provide information which the data controller reasonably expects that the data subject already has; or (b) the provision of such information if it proves impossible or would involve a disproportionate effort.

5.3. Right to object

Consistency with the DIFC Law 2020: Failry consistent

Consistency with the DIFC Law 2007: Fairly inconsistent

The DIFC Law 2020 provides for a broader and more detailed right to object, as well as associated concepts such as consent withdrawal, than the DIFC Law 2007. While there are several similarities between the DIFC Law 2020 and the GDPR, the DIFC Law 2020 does not explicitly discuss fees, response timeframes, and other related matters in the context of the right to object.

GDPR	DIFC Law 2020	DIFC Law 2007
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.	Article 34(1): A data subject has the right to: (a) object at any time on reasonable grounds relating to his particular situation to processing of personal data relating to him where such processing is carried out on the basis that: (i) it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in a controller; or (ii) it is necessary for the purposes of the legitimate interests, where applicable, of a controller or of a third party; and (b) be informed before personal data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object to such disclosures or uses, subject to any provision of this Law that does not permit disclosure; and (c) where personal data is processed for direct marketing purposes, object at any time to such processing, including profiling to the extent that it is related to such direct marketing.	Article 18(1): A data subject has the right: (a) to object at any time on reasonable grounds relating to his particular situation to the processing of personal data relating to him.

GDPR	DIFC Law 2020	DIFC Law 2007
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 32: (1) Where the basis for the processing of personal data is consent under Article 10(1)(a) or under Article 11(1)(a), the data subject may withdraw consent at any time by notifying the controller in accordance with Article 12(5). Where a controller has not complied with Article 12(5) a data subject may notify the controller by any reasonable means. (2) The right to withdraw consent is an absolute right available to a data subject if the basis for the processing of the data subject's personal data is consent under Article 10(1)(a) or Article 11(1)(a). (3) Upon the exercise of a data subject's right to withdraw consent, a controller must comply with Article 22 and must cease processing the personal data as soon as reasonably practicable and ensure that any processors do the same.	The DIFC Law 2007 does not explicitly refer to the withdrawal of consent.
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;	Article 35: (1) Subject to Article 35(3), a data subject shall have the right to require a controller to restrict processing to the extent that any of the following circumstances apply: (a) the accuracy of the personal data is contested by the data subject, for a period allowing 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 its 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;	Article 17: A data subject has the right to obtain from the data controller upon request, at reasonable intervals and without excessive delay or expense: [...] (c) as appropriate, the rectification, erasure or blocking of personal data the processing of which does not comply with the provisions of the Law.

GDPR	DIFC Law 2020	DIFC Law 2007
Restrict Processing (cont'd)		
(d) the data subject has objected to processing pursuant to Article 21(1) pending verification whether the legitimate grounds of the controller override those of the data subject.	(d) the data subject has objected to processing pursuant to Article 34 pending verification of whether the legitimate grounds of the controller override those of the data subject. (2) If a controller lifts the period of restriction it shall inform the data subject in writing. (3) Where Article 35(1) applies, the only processing that may continue to be conducted without the consent of the data subject is: (a) storage of the personal data concerned; (b) processing of the personal data for the establishment, exercise or defence of legal claims; (c) processing for the protection of the rights of another person; and (d) processing for reasons of substantial public interest.	
Object to Direct Marketing		
Article 21(3): Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.	See Article 34(1) above.	Article 18(1): A data subject has the right: [...] (b) to be informed before personal data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object to such disclosures or uses.
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.	Article 29(1): Where personal data has not been obtained from the data subject, a controller shall provide the data subject with at least the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language: [...] (h) any necessary information regarding the specific circumstances in which the personal data is processed, to ensure fair and transparent processing in respect of the data subject, including:	The DIFC Law 2007 does not explicitly provide that data subjects must be informed of the right to object.

GDPR	DIFC Law 2020	DIFC Law 2007
Inform Data Subject of Right (cont'd)		
	[...] (ii) notice 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. Article 34(4): A controller shall, no later than its first communication to a data subject, explicitly bring to the attention of the data subject in clear language that is prominent and separate from other communications or information, the rights referred to in Article 34(1).	
Fees		
See Article 12(5) in section 5.1. above.	The DIFC Law 2020 does not explicitly address this matter in relation to the right to object.	The DIFC Law 2007 does not address fees in relation to the right to object.
Response Timeframe		
See Article 12(3) in section 5.1. above.	The DIFC Law 2020 does not explicitly address this matter in relation to the right to object.	The DIFC Law 2007 does not address response timeframes in relation to the right to object.
Format of Response		
See Article 12(1) in section 5.1. above.	The DIFC Law 2020 does not explicitly address this matter in relation to the right to object.	The DIFC Law 2007 does not address format of responses in relation to the right to object.
Exceptions		
See Article 12(5) in section 5.1. above.	Article 34: (2) Where there is a justified objection, processing initiated by a controller shall no longer include that personal data, and Article 22 shall apply with respect to such personal data. An objection under Article 34(1)(a) is deemed justified unless the controller can demonstrate compelling grounds for such processing that overrides the	The DIFC does not provide specific exceptions to the right to object.

GDPR	DIFC Law 2020	DIFC Law 2007
Exceptions (cont'd)		
	interests or rights of a data subject or that the circumstances in Article 34(3) apply. (3) If a controller collected personal data from a data subject and the controller can demonstrate that the information provided to the data subject under Article 29(1)(h)(ix) was explicit, clear and prominent with respect to the manner of processing the personal data and expressly stated that it would not be possible to implement an objection to the processing at the request of the data subject, then the controller may continue processing the personal data in the same manner, subject to this Law in all other respects.	

5.4. Right of access

Consistency with the DIFC Law 2020: Fairly consistent

Consistency with the DIFC Law 2007: Fairly inconsistent

The DIFC Law 2020 establishes a right of access that is in closer alignment with the GDPR than the DIFC Law 2007. There are still, however, both nuanced and substantive differences between the GDPR and the DIFC Law 2020 including, for instance, the detailing of information that may be accessed.

GDPR	DIFC Law 2020	DIFC Law 2007
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 33(1): Upon request, a data subject has the right to obtain from a controller without charge and within one month of the request: (a) confirmation in writing as to whether or not personal data relating to him is being processed and information at least as to the purposes of the processing, the categories of personal data concerned, and the recipients or categories of recipients to whom the personal data are disclosed; (b) a copy of the personal data undergoing processing in electronic form and of any available information as to its source, including up-to-date information corresponding with the information requirements set out in Articles 29 and 30.	Article 17: A data subject has the right to obtain from the data controller upon request, at reasonable intervals and without excessive delay or expense: (a) confirmation in writing as to whether or not personal data relating to him is being processed and information at least as to the purposes of the processing, the categories of personal data concerned, and the recipients or categories of recipients to whom the personal data are disclosed; (b) communication to him in an intelligible form of the personal data undergoing processing and of any available information as to its source.
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;	See Article 33(1) above.	See Article 17 above.

GDPR	DIFC Law 2020	DIFC Law 2007
Information to be Accessed (cont'd)		
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.		
Inform Data Subject of Right		
See Article 12(1) in section 5.1.	Article 29(1): Where personal data has not been obtained from the data subject, a controller shall provide the data subject with at least the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language: [...] (h) any necessary information regarding the specific circumstances in which the personal data is processed, to ensure fair and transparent processing in respect of the data subject, including: [...] (ii) notice 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.	Article 13: Data controllers shall provide a data subject whose personal data it collects from the data subject with at least the following information as soon as possible upon commencing to collect personal data in respect of that data subject: [...] (c) any further information in so far as such is necessary, having regard to the specific circumstances in which the personal data are collected, to guarantee fair processing in respect of the data subject, such as: [...] (iii) the existence of the right of access to and the right to rectify the personal data.

GDPR	DIFC Law 2020	DIFC Law 2007
Fees		
See Article 12(5) in section 6.1. above.	See Article 33(1) above. Article 33(8): 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, providing written confirmation to the data subject reasons for the refusal.	Article 17 provides that the right to access should be available without 'excessive delay or expense.'
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.	Article 33(10): If a controller has reasonable doubts as to the identity of a data subject asserting a right under this Article 33, it may require the data subject to provide additional information sufficient to confirm the individual's identity. In such cases, the time period for complying with the data subject request does not begin until the controller has received information or evidence sufficient to reasonably identify that the person making the request is the data subject.	The DIFC Law 2007 does not directly address this matter.

GDPR	DIFC Law 2020	DIFC Law 2007
Response Timeframe		
See Article 12(3) in section 6.1. above.	See Article 33(1) above. Article 33(7): If a data subject request under Article 33(1) is particularly complex, or requests are numerous, the controller may send notice to the data subject, within one month, to increase the period for compliance by a further two months citing the reasons for the delay.	Article 17 provides that the right to access should be available without 'excessive delay or expense.'
Format of Response		
See Article 12(1) in section 6.1. above.	Article 33: (11) Where a controller complies with a request under Article 33(1)(b) it shall not disclose the personal data of other individuals in a way that may infringe their rights under applicable law and the controller may redact or otherwise obscure personal data relating to such other individuals. Where the data subject's request is received by electronic means, and unless otherwise requested by the data subject, the information may be provided in a commonly used electronic form. (12) The information to be supplied pursuant to a request under this Article 33 must be supplied by reference to the data in question at the time the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.	The DIFC Law 2007 does not address the format of a response to a data subject access request.

GDPR	DIFC Law 2020	DIFC Law 2007
Exceptions		
See Article 12(5) in section 6.1. above.	Article 33: (8) 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, providing written confirmation to the data subject reasons for the refusal. [...] (13) Without derogating from the requirements on DIFC bodies as set out in Article 65(2), a controller may restrict, wholly or partly, the provision of information to the data subject under Article 33(1) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to: (a) avoid obstructing an official or legal inquiry, investigation or procedure; (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (c) protect public security; (d) protect national security; or (e) protect the rights of others. (14) Where the provision of information to a data subject under Article 33(1) is restricted in accordance with Article 33(13), a controller must inform the data subject in writing without undue delay: (a) that the provision of information has been restricted; (b) of the reasons for the restriction; (c) of the data subject's right to lodge a complaint with the Commissioner under Article 60; and (d) of the data subject's right to apply to the Court under Article 63. (15) Article 33(14)(a) and (b) do not apply to the extent that complying with them would undermine the purpose of the restriction.	The DIFC Law 2007 does not provide specific exceptions to the right to access.

5.5. Right not to be subject to discrimination

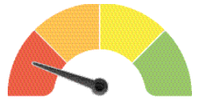
While the DIFC Law 2020 moves into closer alignment with the GDPR than the DIFC Law 2007 in relation to automated processing and the right to object to automated decision-making, there is a marked variation in terms of the right not to be subject to discrimination. Unlike the GDPR or the DIFC Law 2007, the DIFC Law 2020 explicitly defines a right not to be subject to discrimination and associates it with the potential for offering financial incentives for personal data.

GDPR	DIFC Law 2020	DIFC Law 2007
Definition of Right		
The GDPR only implies this right and does not provide an explicit definition for it.	Article 39: (1) A controller may not discriminate against a data subject who exercises any rights under this Part 6, including by: (a) denying any goods or services to the data subject; (b) charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties; (c) providing a less favourable level or quality of goods or services to the data subject; or (d) suggesting that the data subject will receive a less favourable price or rate for goods or services or a less favourable level or quality of goods or services. (2) Nothing in this Article 39 prohibits a controller from charging a data subject a different price or rate, or from providing a different level or quality of goods or services, if that difference is objectively and reasonably directly related to the value provided by the data subject's data. (3) Notwithstanding Article 39(1), a controller may offer financial or non-financial incentives for the processing of personal data provided that: (a) the terms of the incentive are clearly communicated;	The DIFC Law 2007 only implies this right in terms such as 'fair processing' and does not provide an explicit definition for it.

GDPR	DIFC Law 2020	DIFC Law 2007
Definition of Right (cont'd)		
	(b) the process for receiving the benefit of the incentive is clearly communicated, is transparent and does not require material additional effort or expense on the part of the data subject; (c) the nature of the processing involved is clearly communicated; (d) the processing complies in all respects with this Law; and (e) it complies with Article 39(4). (4) A data subject shall have the right to withdraw without penalty from, and require the cessation of processing carried out under, any incentive scheme at any time. Incentive schemes must not be coercive or unreasonable in nature with respect to the processing of personal data, including where the incentive is based on probability or a competition where the chance of receiving the incentive is disproportionately low compared to the value of the personal data and the impact on the data subject's rights.	
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]	Article 38(1): (1) A data subject shall have the right to object to any decision based solely on automated processing, including profiling, which produces legal consequences concerning him or other seriously impactful consequences and to require such decision to be reviewed manually [Article 38 goes on to detail this right, including exceptions].	The DIFC Law 2007 does not provide a right not to be subject to decisions based solely on automated processing.

5.6. Right to data portability

Consistency with the DIFC Law 2020: Fairly consistent



Consistency with the DIFC Law 2007: Inconsistent

Unlike the DIFC Law 2007, the DIFC Law 2020 provides for a right to data portability. This right is in many ways similar to the right to data portability under the GDPR, although there are certain practical differences.

GDPR	DIFC Law 2020	DIFC Law 2007
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.	Article 37(1): A data subject shall have the right to receive personal data that he has provided to a controller in a structured, commonly used and machine-readable format where the processing is: (a) based on the data subject's consent or the performance of a contract; and (b) carried out by automated means.	The DIFC Law 2007 does not provide for a right to data portability.
Inform Data Subject of Right		
See Article 12(1) in section 5.1.	Article 29(1): Where personal data has not been obtained from the data subject, a controller shall provide the data subject with at least the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language: [...] (h) any necessary information regarding the specific circumstances in which the personal data is processed, to ensure fair and transparent processing in respect of the data subject, including: [...] (ii) notice 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.	The DIFC Law 2007 does not provide for a right to data portability.

GDPR	DIFC Law 2020	DIFC Law 2007
Fees		
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 DIFC Law 2020 does not explicitly address this matter in relation to the right to data portability.	The DIFC Law 2007 does not provide for a right to data portability.
Response Timeframe		
See Article 12(3) in section 5.1. above.	The DIFC Law 2020 does not explicitly address this matter in relation to the right to data portability.	The DIFC Law 2007 does not provide for a right to data portability.
Format		
See Article 20(1) above.	See Article 37(1) above.	The DIFC Law 2007 does not provide for a 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.	Article 37(2): The purpose of Article 37(1) is to enable ready portability between controllers if so required by the data subject, and the data subject shall have the right to have the personal data transmitted directly from the controller to whom the request is made to any other person, where technically feasible.	The DIFC Law 2007 does not provide for a right to data portability.
Technically Feasible		
See Article 20(2) above.	See Article 37(2) above.	The DIFC Law 2007 does not provide for a right to data portability.
Exceptions		
See Article 12(5) in section 5.1. above.	Article 37(3): A controller is not required to provide or transmit any personal data where doing so would infringe the rights of any other natural person.	The DIFC Law 2007 does not provide for a right to data portability.

6. Enforcement

6.1. Monetary penalties

Although potential fines have noticeably increased in the DIFC Law 2020 as compared to the DIFC Law 2007, they are still substantially smaller than those provided for under the GDPR. In general, the DIFC Law 2020 remains fairly consistent with the GDPR in terms of establishing monetary penalties that may be issued by the data protection authority, and not providing for sanctions of imprisonment or DPO liabilities.

GDPR	DIFC Law 2020	DIFC Law 2007
Provides for Monetary Penalties		
The GDPR provides for monetary penalties.	The DIFC Law 2020 provides for monetary penalties. [Note: The Regulations 2020 provide further details on the processes of fines.]	The DIFC Law 2007 provides for monetary penalties, which are detailed further in the DPR 2018.
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 62: (2) Subject to Article 62(3), where the Commissioner considers that a controller or processor (including a sub-processor) has contravened the Law, the Commissioner may issue an administrative fine to the controller or processor in respect of a contravention referred to in Schedule 2 in an amount he considers appropriate but not exceeding the amount specified in Schedule 2 in respect of each contravention, payable by the date specified in such notice. (3) The Commissioner may issue a general fine for a contravention of the Law by a controller or processor (including a sub-processor), in an amount he considers appropriate and proportionate, taking into account the seriousness of the contravention and the risk of actual harm to any relevant data subject. Such fine shall be issued by written notice and shall be payable by the date specified in such notice.	Article 36(2): Where the Commissioner of Data Protection considers that a data controller has contravened a provision of the Law referred to in Schedule 2 and in relation to which a fine is stipulated in that Schedule, he may impose by written notice given to the data controller a fine in respect of the contravention, of such amount as he considers appropriate but not exceeding the amount of the maximum fine specified in Schedule 2 in respect of each contravention.

GDPR	DIFC Law 2020	DIFC Law 2007
Fine Maximum		
Article 83(5): infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; (b) the data subjects' rights pursuant to Articles 12 to 22; (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49; (d) any obligations pursuant to Member State law adopted under Chapter IX; (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1). (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.	The maximum fine stipulated within Schedule 2 is for $100,000 (approx. €85,000), which may apply in cases of infringements of data subject rights.	The maximum fine set out in Schedule 2 of the DIFC Law 2007 is $25,000 (approx. €21,000) for failing to register with the Commissioner of Data Protection.
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.	The DIFC Law 2020 does not provide for fines in the amount of a percentage of turnover.	The DIFC Law 2007 does not provide for sanctions that equate to a percentage of turnover.

GDPR	DIFC Law 2020	DIFC Law 2007
Mitigating Factors		
Article 83(2): When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following: (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; (b) the intentional or negligent character of the infringement; (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects; (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32; (e) any relevant previous infringements by the controller or processor; (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; (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;	The DIFC Law 2020 does not explicitly provide general mitigating factors. [Note: the 2020 Regulations provide a template notice for objecting to administrative fines in Appendix 2.]	The DIFC Law 2007 does not specify mitigating factors that may be taken into consideration.

GDPR	DIFC Law 2020	DIFC Law 2007
Mitigating Factors		
(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.	The DIFC Law 2020 does not explicitly provide for imprisonment as a potential sanction.	The DIFC Law 2007 does not explicitly provide for imprisonment as a potential sanction.
DPO Liability		
Not applicable.	The DIFC Law 2020 does not explicitly refer to DPO or individual liabilities.	The DIFC Law 2007 does not explicitly refer to DPO or individual liabilities.

6.2. Supervisory authority

In general terms, the DIFC Law 2020 does not differ significantly from the DIFC Law 2007 in regard to the powers and tasks attributed to the data protection authority. In both cases, they remain substantially similar but less detailed than the equivalent provisions under the GDPR.

GDPR	DIFC Law 2020	DIFC Law 2007
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').	Article 43(1): The President shall appoint a person to be the Commissioner who is appropriately experienced and qualified.	Article 22(1): The President shall appoint a person to be the Commissioner of Data Protection who is appropriately experienced and qualified.
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	Article 46(3): Without limiting the generality of Article 46(1), the Commissioner has the following powers, duties and functions: (a) auditing a controller or processor, which includes having the right to obtain access to any premises and to any processing equipment or means of a controller or processor who is subject to this Law, as well as having the right to require the production of information under Article 52. A controller or processor shall not be required to provide access to or produce legally privileged material or material subject to a conflicting obligation of nondisclosure under Applicable Law. The Commissioner shall seek to minimise unreasonable interruption to the controller or processor in the exercise of its rights under this Article 46(3)(a) and shall give reasonable notice of its access requirements, in each	Article 26: (3) Without limiting the generality of Article 26(1), such powers, duties and functions of the Commissioner of Data Protection shall include, so far as is reasonably practicable: (a) accessing personal data processed by data controllers or data processors; (b) collecting all the information necessary for the performance of its supervisory. [...] (4) The Commissioner of Data Protection has power to do whatever he deems necessary, for or in connection with, or reasonably incidental to, the performance of his functions.

GDPR	DIFC Law 2020	DIFC Law 2007
Investigatory Powers (cont'd)		
controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.	case taking into account the purpose of the audit, the perceived risk to the rights of data subjects, the need to act urgently, the risk of loss or unavailability of information and the seriousness of any suspected contravention of this Law; (b) conducting investigations and inspections to verify compliance with this Law; [...]	
Corrective Powers		
Article 58(2): Each supervisory authority shall have all of the following corrective powers: (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation; (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation; (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation; (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period; (e) to order the controller to communicate a personal data breach to the data subject; (f) to impose a temporary or definitive limitation including a ban on processing; (g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the	Article 46(3): Without limiting the generality of Article 46(1), the Commissioner has the following powers, duties and functions: [...] (c) issuing directions in accordance with Article 59, and issuing warnings or admonishments and making recommendations to a controller or processor, including ordering the appointment of a DPO as described in Article 16(3); (d) initiating proceedings for contraventions of the Law before the Court that may be self-initiated or initiated in response to an investigation of a complaint or a request from a data subject; for such purposes, the Commissioner shall be available for a data subject to contact in order to make complaints and shall take such action as he sees fit in furtherance of his primary objectives described in Article 46(1); (e) imposing fines in the event of non-compliance with a direction; (f) imposing fines for non-compliance with the law and any regulations, including from time to time setting any limits or issuing schedules of fines applicable to specific breaches of the law and any regulations;	Article 26(3): Without limiting the generality of Article 26(1), such powers, duties and functions of the Commissioner of Data Protection shall include, so far as is reasonably practicable: [...] (c) issuing warnings or admonishments and make recommendations to data controllers; (d) initiating proceedings for contraventions of the Law before the Court; (e) imposing fines in the event of non-compliance with its direction; (f) imposing fines for non-compliance with the Laws and any Regulations.

GDPR	DIFC Law 2020	DIFC Law 2007

Corrective Powers (cont'd)

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 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.	(g) initiating a claim for compensation on behalf of a data subject before the Court where there has been a material contravention of the Law to the detriment of the data subject; [...]	

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;	Article 46(3): Without limiting the generality of Article 46(1), the Commissioner has the following powers, duties and functions: [...] (h) preparing or causing to be prepared in a timely and efficient manner: (i) draft regulations; (ii) draft standards or codes of practice; and (iii) guidance; (i) submitting such draft regulations, draft standards, and draft codes of practice to the DIFCA Board of Directors for approval and advising it of any guidance that is issued; (j) promoting, as appropriate, and dealing with codes of conduct intended to contribute towards the application of this Law, as further described in Article 48; (k) prescribing forms to be used for any of the purposes of this Law or any Applicable Law administered by the Commissioner [...]	Article 26(3): Without limiting the generality of Article 26(1), such powers, duties and functions of the Commissioner of Data Protection shall include, so far as is reasonably practicable: [...] (h) preparing or causing to be prepared in a timely and efficient manner: (i) draft Regulations; (ii) draft standards or codes of practice; and (iii) guidance; reasonably required to enable him to perform his statutory functions; (i) submitting such draft Regulations, draft standards, and draft codes of practice to the DIFCA Board of Directors for approval and advising it of any guidance that is issued; (j) prescribing forms to be used for any of the purposes of this Law or any legislation administered by the Commissioner of Data Protection.

GDPR	DIFC Law 2020	DIFC Law 2007

Authorisation/Advisory Powers (cont'd)

(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.		[Note: Article 28 of the DIFC Law 2007 provides for the creation of the DPR 2018.]

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;	Article 46(2): In performing his functions and exercising his powers, the Commissioner shall pursue the following objectives: (a) to monitor, ensure and enforce compliance with this Law; (b) to promote good practices and observance of the requirements of this Law and the Regulations by a controller or processor; and (c) to promote greater awareness and public understanding of data protection and the requirements of this Law and the Regulations in the DIFC.	Article 26(2): In performing his functions and exercising his powers, the Commissioner of Data Protection shall pursue the following objectives: (a) to promote good practices and observance of the requirements of this Law and the Regulations by the data controllers; and (b) to promote greater awareness and public understanding of data protection and the requirements of this Law and the Regulations in the DIFC.

GDPR	DIFC Law 2020	DIFC Law 2007

Tasks of Authority (cont'd)

(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 DPIAs pursuant to Article 35(4);
(l) give advice on the processing operations referred to in Article 36(2);
(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);
(n) encourage the establishment of data protection certification

GDPR	DIFC Law 2020	DIFC Law 2007

Tasks of Authority (cont'd)

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 BCRs 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.

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.

Article 58: (1) Upon request, the Commissioner shall deliver to the President, a report on the management of the administrative affairs of the Commissioner, for the previous year.
(2) Such report shall give a true and fair view of the state of the Commissioner's regulatory operations in the DIFC, and financial statements of the Commissioner, as at the end of the relevant financial year.

Article 32: (1) As soon as practicable after 1 January in each year, the Commissioner of Data Protection shall deliver to the President, a report on the management of the administrative affairs of the Commissioner of Data Protection, for the previous year.
(2) Such report shall give a true and fair view of the state of its regulatory operations in the DIFC, and financial statements of the Commissioner of Data Protection, as at the end of the relevant financial year.

6.3. Civil remedies for individuals

Consistency with the DIFC Law 2020: Fairly consistent

Consistency with the DIFC Law 2007: Fairly consistent

The DIFC Law 2020 establishes slightly more detailed requirements for civil remedies for individuals than the DIFC Law 2007, although they are less comprehensive than the GDPR.

GDPR	DIFC Law 2020	DIFC Law 2007
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 64(1): A data subject who suffers material or non-material damage by reason of any contravention of this Law or the Regulations may apply to the Court for compensation from the controller or processor in question, in addition to, and exclusive of, any fine imposed on the same parties under Article 62. The same measure of damage shall be taken into account in any Court proceeding initiated by the Commissioner under Article 46(3)(d). No person shall be required to pay compensation twice with respect to the same damage.	Article 38: A data subject who suffers damage by reason of any contravention by a data controller of any requirement of this Law or the Regulations may apply to the Court for compensation from the data controller for that damage.
Material and Non-Material Damage		
Article 82(1): Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.	See Article 64(1) above.	The DIFC Law 2007 does not define whether damage can be material and non-material.
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.	Article 46(3): Without limiting the generality of Article 46(1), the Commissioner has the following powers, duties and functions: [..] (g) initiating a claim for compensation on behalf of a data subject before the Court where there has been a material contravention of the Law to the detriment of the data subject.	Article 26(3): Without limiting the generality of Article 26(1), such powers, duties and functions of the Commissioner of Data Protection shall include, so far as is reasonably practicable: [...](g) initiating a claim for compensation on behalf of a data subject before the Court where there has been a material contravention of the Law to the detriment of the data subject.

GDPR	DIFC Law 2020	DIFC Law 2007
Mandate For Representation (cont'd)		
Specifies Amount for Damages		
Not applicable.	The DIFC Law 2020 does not explicitly specify amounts for damages.	The DIFC Law 2007 does not specify an amount for damages.
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.	Article 64: (2) Any controller involved in processing that infringes this Law shall be liable for the damage caused. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Law specifically directed to processors or where it has acted outside or contrary to the lawful instructions of the controller. (3) Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are responsible for any damage caused by processing, each person shall be held jointly and severally liable for the entire damage in order to ensure effective compensation of the data subject.	The DIFC Law 2007 does not define data processor liabilities.
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.	Article 64(4): Proceedings for exercising the right to receive compensation shall be brought before the Court, but may be settled out of Court.	The DIFC Law 2007 does not provide specific exemptions from liabilities.