LATHAM & WATKINS LLP

New Data Protection Law in the DIFC

Who does it apply to and how does it compare with the GDPR?

September 2020

Contents

Introduction

The Dubai International Financial Centre (DIFC) has a new data protection law and regulations: the Data Protection Law DIFC Law No. 5 of 2020 (DIFC DP Law) and the Data Protection Regulations (DIFC DP Regulations, and together with the DIFC DP Law, DIFC DP Legislation).

The DIFC DP Legislation became effective on 1 July 2020, repealing the previous law (Data Protection Law DIFC Law No. 1 of 2007). However, businesses have a grace period of three months (until 1 October 2020) to achieve full compliance.

The Commissioner of Data Protection for the DIFC (Commissioner) has produced a guide to the DIFC DP Legislation (DIFC Guide), which provides a comprehensive overview of the DIFC DP Legislation for entities.

This article aims to:

- Describe who the DIFC DP Legislation applies to
- Map the DIFC DP Legislation against the GDPR and highlight where the DIFC DP Legislation materially differs from the GDPR, taking account of the fact that readers of this article will likely be familiar with the GDPR

Who Does the DIFC DP Legislation Apply To?

Article 6(3) of the DIFC DP Law states that it applies to the following:

1. Businesses incorporated in the DIFC (irrespective of whether the Processing of Personal Data occurs within the DIFC or not)
2. Businesses that Process Personal Data in the DIFC as part of stable arrangements other than on an occasional basis, regardless of their place of incorporation

Point 1 is self-explanatory, but what are "stable arrangements" as contemplated by Point 2? The term is undefined by the DIFC DP Legislation (and therefore open to interpretation in the course of enforcement), but the DIFC Guide explains that stable arrangements can include "a legally binding or recognised agreement or relationship of an existing, valid sort". Readers familiar with the GDPR will recognise this approach, where the legal form is not determinative, as reflective of that taken by the European Data Protection Board's (EDPB's) Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). The Commissioner and the DIFC courts might reasonably be expected to take a similar approach.

How Does the DIFC DP Legislation Compare With the GDPR?

The table on page 3, while not exhaustive, should provide a useful crib sheet for data privacy practitioners familiar with the GDPR to get up to speed on the DIFC DP Legislation. Specifically, the table:

- Sets out the key concepts addressed in the DIFC DP Legislation
- References where those concepts are addressed in both the GDPR and the DIFC DP Legislation
- Notes key differences between how those concepts are addressed in the GDPR and the DIFC DP Legislation where relevant
- Adopts the following colour coding:
    - Bright blue to indicate no material differences between the GDPR and the DIFC DP Legislation
    - Orange to indicate material differences between the GDPR and the DIFC DP Legislation

DIFC DP Legislation vs. GDPR: A Snapshot

Concept	DIFC DP Legislation	GDPR	Comparison between GDPR and DIFC DP Legislation
Key Definitions:			
Personal Data	Paragraph 3 *(Defined terms)*, Schedule 1 of the DIFC DP Law	Article 4(1) *(Definitions)*	The definition of Personal Data in the DIFC DP Law is materially the same as the definition in the GDPR.
Identifiable Natural Person	Paragraph 3 *(Defined terms)*, Schedule 1 of the DIFC DP Law	Article 4(1) *(Definitions)*	The definition of Identifiable Natural Person in the DIFC DP Law is materially the same as the definition in the GDPR.
Special Category Data	Paragraph 3 *(Defined terms)*, Schedule 1 of the DIFC DP Law	Article 9 *(Processing of special categories of personal data)*	The definition of Special Category Data differs in the DIFC DP Law. In addition to including the categories of Personal Data that the GDPR identifies as sensitive, the DIFC DP Law also includes references to "communal origin" and "political affiliations" (as opposed to political opinions as set forth in Article 9 of the GDPR). However, unlike the GDPR, this definition does not include a reference to "sexual orientation".
Processing	Paragraph 3 *(Defined terms)*, Schedule 1 of the DIFC DP Law	Article 4(2) *(Definitions)*	The definition of Processing in the DIFC DP Law is materially the same as the definition in the GDPR.
High Risk Processing Activities	Paragraph 3 (*Defined terms)*, Schedule 1 of the DIFC DP Law	N/A	Unlike the GDPR, the DIFC DP Law defines High Risk Processing Activities. High Risk Processing Activities refers to Processing Personal Data where one or more of the following applies: (i) 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 their rights. (ii) A considerable amount of Personal Data will be Processed, and such Processing is likely to result in a high risk to the Data Subject.

Concept **Key Definitions:**	DIFC DP Legislation	GDPR	Comparison between GDPR and DIFC DP Legislation
			(iii) 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. (iv) A material amount of Special Categories of Personal Data is to be Processed. The DIFC DP Law's definition of High Risk Processing Activities is largely consistent with the nature of activities identified in the EDPB Guidelines on Data Protection Impact Assessment (DPIA) and determining whether Processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, and therefore, for practical purposes, the definition of High Risk Processing Activities is materially the same as the "definition" in the aforementioned guidelines.
Data Subject	Paragraph 3 *(Defined terms)*, Schedule 1 of the DIFC DP Law	Article 4(1) *(Definitions)*	The definition of Data Subject in the DIFC DP Law is materially the same as the definition in the GDPR.
Controller	Paragraph 3 (*Defined terms)*, Schedule 1 of the DIFC DP Law	Article 4(7) *(Definitions)*	The definition of Controller in the DIFC DP Law is materially the same as the definition in the GDPR.
Joint Controller	Paragraph 3 *(Defined terms)*, Schedule 1 of the DIFC DP Law	Article 26 *(Joint controllers)*	The definition of Joint Controller in the DIFC DP Law is materially the same as the definition in the GDPR.
Processor	Paragraph 3 *(Defined terms)*, Schedule 1 of the DIFC DP Law	Article 4(8) *(Definitions)*	The definition of Processor in the DIFC DP Law is materially the same as the definition in the GDPR.
Sub-processor	Paragraph 3 *(Defined terms)*, Schedule 1 of the DIFC DP Law	N/A	Unlike the GDPR, the DIFC DP Law defines Sub-processor; however, Latham understands this to be a commonly understood term within data privacy jurisprudence.

Concept	DIFC DP Legislation	GDPR	Comparison between GDPR and DIFC DP Legislation
Requirements for Legitimate and Lawful Processing	Article 9 *(General requirements)* of the DIFC DP Law Article 10 *(Lawfulness of Processing)* of the DIFC DP Law	Article 6 *(Lawfulness of processing)* Recitals 39 to 50	No material differences — the DIFC DP Law provides essentially the same legal bases for Processing Personal Data as the GDPR.
Processing of Special Categories of Personal Data	Article 11 *(Processing of Special Categories of Personal Data)* of the DIFC DP Law	Article 9 *(Processing of special categories of personal data)* Recitals 46 and 51 to 56	The DIFC DP Law differs from the GDPR. In addition to the conditions in the GDPR where Special Categories of Personal Data may be Processed, the DIFC DP Law also contains the following derogations: (i) Processing that is proportional and necessary to protect Data Subjects from potential bias or inaccurate decision-making. (ii) Protecting members of the public against dishonesty, malpractice, incompetence or other improper conduct of persons providing banking, insurance, investment, management consultancy, information technology services, accounting, or other services or commercial activities. Note that the GDPR also permits Member States to introduce additional conditions, including limitations, on the Processing of Special Categories of Personal Data.
Meaning of Consent	Article 12 *(Consent)* of the DIFC DP Law	Article 7 *(Conditions for consent)* Article 8 *(Conditions applicable to child's consent in relation to information society services)*	The DIFC DP Law differs from the GDPR. In addition to the GDPR's standard of consent, i.e., that the consent be freely given, specific, and demonstrated by a clear affirmative act showing an unambiguous indication of consent, the DIFC DP Law also requires that: (i) The Controller should implement appropriate and proportionate measures to assess the ongoing validity of consent.

Concept	DIFC DP Legislation	GDPR	Comparison between GDPR and DIFC DP Legislation
		Recitals 32, 33, 38, 42 and 43	(ii) Where such assessment concludes that a Data Subject would no longer reasonably expect the Processing to be continuing, the Data Subject is contacted without delay and asked to re-affirm its consent. For further information on the elements of consent under the DIFC DP Legislation, see the Commissioner's Guidance relating to Data Subject Consent.
Reliance on Legitimate Interests	Article 13 *(Legitimate interests)* of the DIFC DP Law	Article 6(1)(f) *(Lawfulness of processing)* Recitals 47 and 48	The DIFC DP Law differs from the GDPR. Article 13(1) of the DIFC DP Law specifies that a public authority may not rely on legitimate interests to Process Personal Data. Article 6(1)(f) of the GDPR specifies that a public authority may not rely on legitimate interests to Process Personal Data in performance of its tasks. This suggests that under the DIFC DP Law, a public authority may not rely on legitimate interests at all, whereas under the GDPR, a public authority may rely on legitimate interests if it is performing tasks other than in its capacity as a public authority, e.g., pursuing commercial interests.
Accountability and Notification	Article 14 *(Accountability and notification)* of the DIFC DP Law	Article 24 *(Responsibility of the controller)* Article 25 *(Data protection by design and by default)* Recitals 74 to 78	No material differences — both the DIFC DP Law and the GDPR specify that Controllers are required to put in place programs demonstrating compliance with the respective laws.
Records of Processing	Article 15 *(Records of Processing activities)* of the DIFC DP Law	Article 30 *(Records of processing activities)* Recitals 13 and 82	No material differences — both the DIFC DP Law and the GDPR specify that Controllers and Processors are required to maintain a written record of their Processing activities.

Concept	DIFC DP Legislation	GDPR	Comparison between GDPR and DIFC DP Legislation
Appointment and Role of Data Protection Officer	Article 16 *(Designation of the DPO)* of the DIFC DP Law Article 17 *(The DPO: competencies and status)* of the DIFC DP Law Article 18 *(Role and tasks of the DPO)* of the DIFC DP Law Article 19 *(DPO Controller assessment)* of the DIFC DP Law	Article 37 *(Designation of the data protection officer)* Article 38 *(Position of the data protection officer)* Article 39 *(Tasks of the data protection officer)* Recital 97	The DIFC DP Law differs from the GDPR. The DIFC DP Law requires a Data Processing Officer (DPO) to be appointed by a Controller or Processor performing "High Risk Processing Activities" on a systematic or regular basis. Article 37(1) of the GDPR specifies that a Controller or Processor shall designate a DPO if: (i) The Processing is carried out by a public body (except for courts acting in their judicial capacity). (ii) The core activities of the Controller or Processor require large-scale, regular, and systematic monitoring of individuals. (iii) The core activities of the Controller or Processor consist of Processing sensitive personal data or data relating to criminal convictions and offences on a large scale. Under the DIFC DP Law, the appointment of a DPO is required in similar situations to that in Article 37(1) of the GDPR. However, the DIFC DP Law also requires the appointment of a DPO if Processing 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. The DIFC DP Law also states that even if a business is not required to appoint a DPO, it must still allocate responsibility for data protection oversight and compliance, and be able to provide details of the persons with such responsibility to the Commissioner.

Concept	DIFC DP Legislation	GDPR	Comparison between GDPR and DIFC DP Legislation
Privacy Impact Assessments	Article 20 *(Data protection impact assessment)* of the DIFC DP Law	Article 35 *(Data protection impact assessment)* Recitals 75, 84 and 89 to 93	The DIFC DP Law differs from the GDPR. Although the DIFC DP Law requires a Privacy Impact Assessment (PIA) in materially the same situations as the GDPR does, the DIFC DP Law does not contain an express requirement for a PIA if there is a systematic monitoring on a large scale. However, it is arguable (and suggested in the Commissioner's guidance on High Risk Processing Activities) that this requirement may fall within the definition of High Risk Processing Activities, and therefore require a PIA.
Consultation With Authority Prior to Processing	Article 21 *(Prior consultation)* of the DIFC DP Law	Article 36 *(Prior consultation)* Recitals 94 to 96	The DIFC DP Law differs from the GDPR. The DIFC DP Law specifies that, following a consultation, the Commissioner may make a direction with respect to a Processing activity, and the Controller shall implement such direction without delay. Under the GDPR, the trigger point for a supervisory authority to issue a similar direction is if the supervisory authority thinks that the intended processing infringes the GDPR.
Cessation of Processing	Article 22 (*Cessation of Processing*) of the DIFC DP Law	Article 5(1)(e) Recital 39	The DIFC DP Law differs from the GDPR. 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, Controllers are offered alternatives to deletion, e.g., pseudonymisation or encryption. Under the GDPR, this is not permitted and Controllers must adhere to the storage limitation principle.
Binding Agreements for Joint Controllers	Article 23 *(Joint Controllers)* of the DIFC DP Law Article 64 *(Compensation)* of the DIFC DP Law	Article 26 *(Joint controllers)* Article 82 *(Right to compensation and liability)* Recitals 58, 79, 146 and 147	The DIFC DP Law differs from the GDPR. The DIFC DP Law does not include an equivalent to Article 82(5) of the GDPR, which provides that a Controller or Processor held to be fully liable for any damage caused in Processing is entitled to claim back from the other Controllers or Processors involved in the same Processing that part of the compensation corresponding to their part of responsibility for the damage.

Concept	DIFC DP Legislation	GDPR	Comparison between GDPR and DIFC DP Legislation
Binding Agreements for Processors and Sub-Processors	Article 24 *(Processors and Sub-processors)* of the DIFC DP Law	Article 28 *(Processor)* Recital 81	No material differences — the DIFC DP Law has largely incorporated the same Controller-to-Processor contract requirements.
Transfers Out of Jurisdiction if There Is an Adequate Level of Protection	Article 26 *(Transfers out of the DIFC: adequate level of protection)* of the DIFC DP Law Appendix 3 *(Adequate Jurisdictions)* of the DIFC DP Regulations	Article 45 *(Transfers on the basis of an adequacy decision)* Recitals 103 to 107	The Commissioner and the European Commission (EC) have not deemed the same jurisdictions as having an adequate level of protection for Personal Data as each other. For example: (i) The EC has recognised Israel as an adequate jurisdiction whereas the Commissioner has not. (ii) The Commissioner has recognised the Abu Dhabi Global Market as an adequate jurisdiction whereas the EC has not. See the DIFC's list of adequate jurisdictions.
Transfers Out of Jurisdiction if There Is Not an Adequate Level of Protection	Article 27 *(Transfers out of the DIFC in the absence of an adequate level of protection)* of the DIFC DP Law	Article 46 *(Transfers subject to appropriate safeguards)* Recitals 108 and 109	No material differences — the DIFC DP Law and the GDPR provide similar mechanisms (standard contractual clauses, binding corporate rules etc.) which permit the transfer of data in the absence of an adequate level of protection. The European Court of Justice has invalidated the EU-US Privacy Shield and imposed significant conditions on the use of the standard contractual clauses/ model clauses. For further detail, see this Latham blog post.

Concept	DIFC DP Legislation	GDPR	Comparison between GDPR and DIFC DP Legislation
Sharing Data With Other Public Authorities	Article 28 *(Data sharing)* of the DIFC DP Law	Article 48 *(Transfers or disclosures not authorised by Union law)* Recital 115	The DIFC DP Law differs from the GDPR. The DIFC DP Law permits the transfer or disclosure of Personal Data in a broader number of circumstances than the GDPR does, where a Controller or Processor, having received a request for disclosure from a public authority, has taken reasonable steps to satisfy itself that: (i) The request from the public authority is a valid and proportionate request. (ii) The requesting authority will respect the rights of Data Subjects in Processing their Personal Data.
Transparency Obligations	Article 29 (*Providing information where Personal Data has been obtained from the Data Subject)* of the DIFC DP Law Article 30 *(Providing information where Personal Data has not been obtained from the Data Subject)* of the DIFC DP Law Article 31 *(Nature of Processing information)* of the DIFC DP Law	Article 13 *(Information to be provided where personal data are collected from the data subject)* Article 14 *(Information to be provided where personal data have not been obtained from the data subject)* Recitals 60 to 62	The DIFC DP Law differs from the GDPR. In addition to the information that needs to be provided to a Data Subject, where the Controller has obtained Personal Data directly from the Data Subject, under the DIFC DP Law the Controller shall also provide the following information (insofar as it 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): (i) Whether replies to questions are obligatory or voluntary, as well as the possible consequences of failure to reply. (ii) Whether Personal Data will be used for direct marketing purposes. (iii) If the Controller intends to Process Personal Data in a manner that will restrict or prevent the Data Subject from exercising their rights to request rectification, erasure, or object to Processing, an explanation of the expected impact on such rights (the Controller shall also satisfy itself that the Data Subject understands the extent of those restrictions).

Concept	DIFC DP Legislation	GDPR	Comparison between GDPR and DIFC DP Legislation
Rights of Data Subjects	Article 32 *(Right to withdraw consent)* of the DIFC DP Law Article 33 *(Right to access, rectification and erasure of Personal Data)* of the DIFC DP Law Article 34 *(Right to object to Processing)* of the DIFC DP Law Article 35 *(Right to restriction of Processing)* of the DIFC DP Law Article 37 *(Right to data portability)* of the DIFC DP Law Article 38 *(Automated individual decision-making, including Profiling)* of the DIFC DP Law Article 39 *(Non-discrimination)* of the DIFC DP Law Article 40 *(Methods of exercising Data Subject rights)* of the DIFC DP Law	Article 12 (*Transparent information, communication and modalities for the exercise of the rights of the data subject)* to Article 22 (*Automated individual decision-making, including profiling)* Recitals 58 to 73 and 91	The DIFC DP Legislation differs from the GDPR. In addition to the rights that Data Subjects have under the GDPR, Data Subjects also have the right not to be discriminated against when they exercise their rights under Part 6 *(Rights of Data Subjects)* of the DIFC DP Law. For example, if a Data Subject exercises their rights under Part 6 *(Rights of Data Subjects)* of the DIFC DP Law, a Controller may not (purely as a result of the Data Subject having exercised such rights): (i) Deny any goods or services to that Data Subject. (ii) Charge different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties. (iii) Provide a less favourable level or quality of goods or services to that Data Subject. (iv) Suggest 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.

Concept	DIFC DP Legislation	GDPR	Comparison between GDPR and DIFC DP Legislation
Personal Data Breaches — Notification to Commissioner	Article 41 *(Notification of Personal Data Breaches to the Commissioner)* of the DIFC DP Law	Article 33 *(Notification of a personal data breach to the supervisory authority)* Recitals 85, 87 and 88	The DIFC DP Law differs from the GDPR with regards to when a Controller is required to notify the Commissioner in the event of a Personal Data Breach. The DIFC DP Law specifies that Personal Data Breaches should be notified to the Commissioner "as soon as practicable" whereas a GDPR controller's obligation is to notify a data breach to a supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it".
Personal Data Breaches — Notification to Data Subjects	Article 42 *(Notification of Personal Data Breaches to a Data Subject)* of the DIFC DP Law	Article 34 *(Communication of a personal data breach to the data subject)* Recitals 86, 87 and 88	No material differences — the time period for reporting Personal Data Breaches to the Data Subject is largely the same in the DIFC DP Law ("as soon as practicable in the circumstances") and the GDPR ("without undue delay") as there is no 72-hour deadline for notifying data subjects under the GDPR.
Enforcement Powers of Authority — Non-Monetary	Article 46 *(Powers, functions and objectives of the Commissioner)* of the DIFC DP Law Article 59 *(Directions)* of the DIFC DP Law	Article 58 *(Powers)* Recitals 122, 129 and 131	No material differences — the DIFC DP Law and the GDPR afford the Commissioner and supervisory authority in each Member State broad powers to enforce the application of the respective laws.
Enforcement Powers of Authority — Fines	Article 62 *(Imposition of Fines)* of the DIFC DP Law Schedule 2 of the DIFC DP Law	Article 82 *(Right to compensation and liability)* Article 83 *(General conditions for imposing administrative fines)* Recitals 146 to 152	The DIFC DP Legislation differs from the GDPR. The maximum applicable administrative fines under the DIFC DP Legislation are much lower than under the GDPR, and will not exceed US$100,000. Notably, the list of fines in the DIFC DP Law is not exhaustive, and may be updated from time to time. The DIFC DP Law also states that the Commissioner may issue a general fine (not subject to a cap) for a contravention of the DIFC DP Law by a business, "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".

Concept	DIFC DP Legislation	GDPR	Comparison between GDPR and DIFC DP Legislation
Other Remedies of Data Subjects	Article 60 *(Lodging complaints and mediation)* of the DIFC DP Law Article 63 *(Application to the Court)* of the DIFC DP Law Article 64 *(Compensation)* of the DIFC DP Law	Article 77 *(Right to lodge a complaint with a supervisory authority)* Article 78 *(Right to an effective judicial remedy against a supervisory authority)* Article 79 *(Right to an effective judicial remedy against a controller or processor)* Article 82 *(Right to compensation and liability)* Recitals 141, 143 and 145 to 147	No material differences — the DIFC DP Law and the GDPR afford Data Subjects similar rights, e.g., allowing them to make compensation claims in relation to contraventions of the relevant laws.

Practical Takeaways

Any entity subject to the DIFC DP Legislation should:

- Understand the impact of the changes and obligations under the DIFC DP Legalisation
- Conduct an audit of its Processing activities
- Consider the appointment of a DPO as a general requirement, and proceed to appoint a DPO when performing High Risk Processing Activities on a systematic or regular basis
- Ensure that it has the right procedures in place to (i) support Data Subjects' rights; and (ii) detect, report, and investigate a Personal Data Breach within the prescribed timelines
- Review and update its (i) privacy notice; (ii) consent forms; and (iii) contracts with Joint Controllers, Processors, and Sub-processors to ensure that they reflect the mandatory requirements
- Notify its employees of the requirements under the DIFC DP Legislation
- Create a record of its Processing activity under this responsibility
- Review (i) international transfers of Personal Data to ensure that transfers are made in accordance with DIFC DP Legislation; and (ii) the legal bases currently adopted for Processing Personal Data, including Special Categories of Personal Data
- Conduct a privacy impact assessment, prior to undertaking a High Risk Processing Activity

Conclusion

The DIFC DP Legislation is similar to the GDPR in many respects, but there are important differences, including (i) the possibility for Controllers and Processors to continue to use Personal Data in encrypted or pseudonymised form after the legal basis for Processing has ceased; (ii) the timeline for reporting Personal Data Breaches to the Commissioner; (iii) the maximum applicable administrative fines; (iv) additional "special category" data categories; (v) inclusion of measures to assess the validity of consent; and (vi) the prohibition on discrimination. On the whole the DIFC DP Legislation is a welcome development for the DIFC and sets a new and significant benchmark for data privacy in the Middle East.

Contacts

Data & Technology Transactions

Brian A. Meenagh
Partner, Dubai
T +971.4.704.6344
E brian.meenagh@lw.com

Fiona M. Maclean
Partner, London
T +44.20.7710.1822
E fiona.maclean@lw.com

Alexander Hendry*
Associate, Dubai
T +971.4.704.6385
E alexander.hendry@lw.com

Avinash Balendran
Associate, Dubai
T +971.4.704.6300
E avinash.balendran@lw.com

** Admitted to practice in Scotland*