SQUIRE PATTON BOGGS

Data Protection Under the New Dubai International Financial Centre Data Protection Law

Comparative Overview of GDPR and the DIFC Data Protection Law 2020

The Dubai International Financial Centre (DIFC) Market is one of the two common law financial free zones in the United Arab Emirates (UAE). Established in 2004, it is the oldest such free zone and the largest, currently contributing just under 4% of Dubai's GDP.

The DIFC has its own commercial legal regime, based upon and incorporating aspects of English law, distinct from the laws of the UAE and the Emirates, and its own legislative authority. Financial services are regulated and overseen by a regulator – the Dubai Financial Services Authority – modelled on the UK's Financial Conduct Authority (FCA). It also boasts its own court system, consisting of a Court of First Instance and a Court of Appeal. Legal mechanisms exist that permit the enforcement of the judgments of these courts in the "mainland" UAE and internationally.

The new DIFC Data Protection Law, Law No. 5 of 2020 (DIFC DP Law) came into force on 1 July 2020 and will be enforced from 1 October 2020. The new law, which repeals the Data Protection Law No.1 of 2007, applies to the processing of data by controllers or processors incorporated in the DIFC, irrespective of whether the processing takes place in the DIFC. It also applies to controllers or processors that process personal data in the DIFC on a regular basis, regardless of the entity's place of incorporation.

Unlike with the EU General Data Protection Regulation (GDPR), where companies had a two-year transition period to become compliant, there has not been much time for DIFC entities to prepare for compliance with the new DIFC DP Law. With the date of enforcement around the corner, it is important for companies, branches and other legal entities operating in the DIFC to take the time to achieve reasonable compliance with the new law. The fines for non-compliance are relatively high (even if lower than GDPR penalties), with maximum thresholds starting at US$10,000 and going up to US$100,000 depending on the contravention in question.

The new DIFC DP Law draws heavily on the GDPR. The two can almost be read side by side. As with the GDPR, the DIFC DP Law:

- Requires records of processing to be kept
- Incorporates the concepts of "controllers" and "processors" of data, as well as "joint controllers"
- Establishes lawful bases required for processing, including consent, but also providing for five additional bases
- Introduces general requirements for processing data comparable to the principles contained in the GDPR
- Requires Data Protection Impact Assessments (DPIAs) to be carried out for "high-risk" processing
- Grants data subjects rights on a par with those granted by the GDPR
- Grants data subjects the right to seek compensation where they have suffered damage as the result of an infringement of the law
- Prohibits international transfers unless there are appropriate safeguards in place
- Sets out the criteria for determining when an entity must appoint a data protection officer (DPO)

A side-by-side comparison of key provisions of the two laws is provided below.

Contacts

If you require assistance in relation to the new DIFC DP Law, please reach out to your usual contact at the firm or any of the following members of our DIFC DP Law task force:

Rosa Barcelo
Co-Chair, Data Privacy & Cybersecurity Practice
Partner, Brussels
T +322 627 1107
E rosa.barcelo@squirepb.com

Ann Lafrance
Co-Chair, Data Privacy & Cybersecurity Practice
Partner, New York
T +1 212 872 9830
E ann.lafrance@squirepb.com

Douglas Smith
Partner, Dubai
T +971 4 447 8737
E douglas.smith@squirepb.com

Campbell Steedman
Partner, Dubai
T +971 4 447 8760
E campbell.steedman@squirepb.com

Asel Ibraimova
Associate, London
T +44 207 655 1208
E asel.ibraimova@squirepb.com

Habib Saeed
Associate, Dubai
T +971 4 447 8736
E habib.saeed@squirepb.com

How We Can Help

Our DIFC DP Law task force includes data protection experts combining DIFC data protection and general legal experience with extensive GDPR experience.

Our team is available to assist with practical implementation support and to help leverage our clients' GDPR compliance work in the DIFC context.

Among the tasks that we can assist with are the following:

- Implementing records of processing and helping identify compliance gaps – we have developed comprehensive mapping documents for you to use
- Reviewing and redrafting privacy notices to include the new information requirements of the DIFC law
- Putting in place mechanisms for obtaining explicit data subject consents where required
- Evaluating whether processing qualifies as "high risk" and, thus, triggering the requirement for DPIAs; and assisting with DPIAs for specific processing activities
- Drafting and future-proofing new agreements with service providers, including reviewing how liability is allocated
- Helping you assess the adequacy of the security arrangements of your service provider processors, including providing security compliance checklists
- Advising on the measures available to legitimise transfers of personal data outside of the DIFC and documenting the same
- Assisting you to create a robust data breach incident response plan (IRP), or integrate the DIFC DP Law into your existing IRP
- Developing data subject access processes and advising on platforms that will enable your organisation to respond to requests
- Advising you on whether the DPO requirement applies to your organisation
- Assessing and advising on the application of controller, joint controller and processor status
- Providing education and training on data protection issues for all stakeholders in your organisation

Comparison of Key Provisions of the GDPR and the DIFC Data Privacy Law

	GDPR	DIFC DP Law
Definition of "Personal Data"	**Article 4** 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".
Definition of "Special Categories of Personal Data"	**Article 9** "…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".	**Defined in Article 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."

	GDPR	DIFC DP Law
Principles	**Article 5** Personal data shall be: (a) **Processed lawfully, fairly and in a transparent manner** in relation to the data subject ('lawfulness, fairness and transparency'); (b) 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'); (c) Adequate, **relevant and limited to what is necessary in relation to the purposes** for which they are processed ('data minimisation'); (d) **Accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); (e) **Kept in a form that permits identification of data subjects for no longer than is necessary** for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); (f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). • Consent • Necessary for performance of a contract • Necessary for compliance with legal obligation • Necessary to protect vital interests of a data subject • Necessary for performance of a task carried out in the public interest or in the exercise of official authority • Necessary for the purposes of legitimate interests	**Article 9(1)** Personal Data shall be: (a) Processed in accordance with Article 10; (b) **Processed lawfully, fairly and in a transparent manner** in relation to a Data Subject; (c) Processed for **specified, explicit and legitimate purposes** determined at the time of collection of Personal Data; (d) Processed in a way that is not incompatible with the purposes described in Article 9(1)(c); (e) **Relevant and limited to what is necessary in relation to the purposes** described in Article 9(1)(c); (f) Processed in accordance with the application of Data Subject rights under this Law; (g) **Accurate and, where necessary, kept up to date**, including via erasure or rectification, without undue delay; (h) **Kept in a form that permits identification of a Data Subject for no longer than is necessary** for the purposes described in Article 9(1)(c); and (i) Kept **secure**, including being protected **against unauthorised or unlawful Processing** (including transfers), **and against accidental loss, destruction or damage, using appropriate technical or organisational measures**.
Legal Bases for Processing	• Consent • Necessary for performance of a contract • Necessary for compliance with legal obligation • Necessary to protect vital interests of a data subject • Necessary for performance of a task carried out in the public interest or in the exercise of official authority • Necessary for the purposes of legitimate interests	• Consent • Necessary for performance of a contract • Necessary for compliance with applicable law • Necessary to protect vital interests of a data subject • Necessary for performance of a task carried out by a DIFC Body or to exercise a DIFC Body's powers • Necessary for the purposes of legitimate interests

	GDPR	DIFC DP Law
Data Subjects' Rights	**Articles 15-22, 77** • Right of access • Right to rectification • Right to erasure • Right to restriction of processing • Right to data portability • Right to object • Right not to be subject to decisions based solely on automated processing, including profiling	**Articles 32-40** • Right to access, rectification and erasure • Right to withdraw consent • Right to object to processing • Right to restriction of processing • Right to data portability • Automated individual decision-making, including profiling • Non-discrimination
Consent	**Article 7** "… 2. If the data subject's consent is given in the context of a written declaration … the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language… 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. 4. When assessing whether consent is **freely given**, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."	**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." Similar to the GDPR, the controller must be able to demonstrate that the consent has been freely given and that consent can be withdrawn by the data subject at any time. Unlike the GDPR, DIFC law specifically states that the controller must assess the ongoing validity of consent and where the results of that analysis suggest that the consent may not be ongoing, the data subject should be contacted. The standard of consent under the 2007 Law does not satisfy the new requirements and will likely need to be re-sought in order to be compliant with the new law.
Breach Notification	**Article 33** "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** "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."
Fines/Penalties for Non-Compliance	Fines of up to €20 million or 4% of annual global turnover.	Fines vary from US$10,000 to US$100,000.

	GDPR	DIFC DP Law
Obligation to Keep Records of Processing	**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 (subject to authorised measures) the documentation of suitable safeguards**."	**Article 2.1** "For the purposes of Article 15(1) of the Law, 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 Protection Impact Assessments (DPIAs)	**Article 35** "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…" Processing: • Systematic and extensive evaluation of personal data based on automated processing, including profiling, and on which decisions are based that produce legal or similarly significant effects concerning individuals • Processing large scale of special categories of data or of personal data relating to criminal records • Systematic monitoring of a publicly accessible area on a large scale	**Article 20** "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." Processing: • High risk, new/different technologies AND Increased risk to the security/rights of a data subject • Considerable amount of personal data likely to result in a high risk to the data subject, due to sensitivity or risks • Automated processing • Material amount of special categories
Agreements	Both require agreements between controllers and processors with certain mandatory provisions/obligations.	Both require agreements between controllers and processors with certain mandatory provisions/obligations.
International Transfers	The GDPR only allows for international transfers of data subject to certain safeguards set out in the Regulation, including: • Transfers to a country or territory approved by the Commission via an adequacy decision; • A legal binding instrument between public authorities; • Binding corporate rules; or • Standard data protection clauses adopted by the Commission.	As with the GDPR, the DIFC Law only allows for international transfers of data outside DIFC if certain safeguards are in place. These safeguards include: • A legal binding instrument between public authorities; • Binding corporate rules; or • Standard data protection clauses adopted by the Commissioner.

	GDPR	DIFC DP Law
Privacy Notices	**Articles 13-14** Both the GDPR and the DIFC DP Law set out information to be provided where personal data are collected from the data subject and where personal data have been obtained from a source other than the data subject. Information to be provided to data subjects under the GDPR includes: • **The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;** • **The existence of the right to request 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 right to withdraw consent at any time;** • **The right to lodge a complaint with a supervisory authority;** • **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 the possible consequences of failure to provide such data; and** • **If applicable, the existence of automated decision-making, including profiling and at least meaningful information about the logic involved and the significance and envisaged consequences of such processing for the data subject.**	**Articles 29-30** Information to be provided to data subjects includes: • **The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;** • **The existence of the right to request 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 right to withdraw consent at any time;** • **The right to lodge a complaint with the Commissioner;** • **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;** • **If applicable, the existence of automated decision-making, including profiling;** • **Whether replies to questions are obligatory or voluntary, as well as the possible consequences of failure to reply;** • Whether the Personal Data will be used for direct marketing purposes; and • 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.
Data Protection Officer (DPO)	**Articles 37-39** "1. The controller and the processor shall designate a data protection officer in any case where: (a) The processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) The core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10."	**Articles 16-19** As under the GDPR, a DPO is required under specified circumstances, although these circumstances differ slightly. Note, the appointed DPO must reside in the UAE, unless he/she is employed within an organisation's group (i.e. a subsidiary of a parent company) and performs a similar function within that organisation on an international basis. There are no such restrictions on the residency of the DPO in the GDPR. A DPO shall be appointed by a Controller or Processor performing "High Risk Processing Activities" on a systematic regular basis. "High Risk Processing Activities" is defined as Processing of Personal Data where one 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;** (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**".

	GDPR	DIFC DP Law
Private Right of Action	**Articles 77-84** The GDPR grants data subjects the ability to seek a private right of action. Any person who has suffered damage, whether material or non-material, as a result of an infringement of the GDPR has the right to receive compensation from the controller or processor for the damage suffered.	**Article 64** Following the GDPR, the DIFC law also grants data subjects the right to seek compensation. "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."