



Data Privacy Frameworks in MENA

Emerging approaches and common principles

November 2019



The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.

For more information, please visit the GSMA corporate website at www.gsma.com and MENA regional website at www.gsma.com/mena

Follow the GSMA on Twitter: [@GSMA](https://twitter.com/GSMA)



Established in the UAE for 40 years, PwC has more than 5,200 people in 12 countries across the region: Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Oman, the Palestinian territories, Qatar, Saudi Arabia and the United Arab Emirates. We partner with our region's governments and businesses, to help solve the region's most important problems and build trust in our society. We are investing in the very best talent, providing an unparalleled range of expert capabilities from Legal, through Advisory and Consulting to Tax, Strategy, Digital Trust and Assurance Services, underpinned by the standout digital platform in the region.

Table of Contents

Jurisdiction	Page
Glossary	4
Executive summary	5
Scope	8
Jurisdictional overview	9
Jurisdictional GDPR alignment	11
United Arab Emirates	12
UAE Free Zones	32
Saudi Arabia	53
Saudi Cloud Computing Regulatory Framework	72
Jordan	78
Kuwait	94
Egypt	113
Oman	132
Bahrain	151

Jurisdiction	Page
Lebanon	168
Qatar	183
Qatar Financial Centre	203
Turkey	220

Glossary

Term	Meaning
1995 Directive	Data Protection Directive (95/46/EC).
Cross-border data transfers	any transfer of Personal Data which are undergoing Processing or are intended for Processing after transfer to a another country.
Data controller	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.
Data processor	the natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.
Data subject	any information relating to an identified or identifiable natural person.
DPSA	data protection supervisory authority.
GDPR	General Data Protection Regulation (2016/679/EU).
Processing	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.

Executive summary

Importance of privacy and data protection frameworks

The increase in global data privacy regulations and both public and media awareness of data sharing and ownership are creating new challenges and opportunities that impact consumers and businesses globally.

In today's world, the value of data as a strategic asset and powerful source of economic value is clear.¹ New business models are built on data and data science and analytics. To protect consumers' privacy, and to support their own new data-driven business models, businesses need to appropriately manage and secure their data. New regulatory requirements confirm this importance, whether for personal or non-personal data. The misuse or mismanagement of data can strongly influence the public perception of an organisation in the market. Conversely, an organisation can also gain competitive advantage and customer trust through 'data protection by design' and 'by default' principles, privacy-enhancing technologies and accountability measures. These are some of the many benefits of putting appropriate privacy frameworks in place.

One of the other benefits is that implementing consistent, principles-based, risk-based, horizontal privacy frameworks at the national level can create the right conditions for data sharing across a region, leading to regional economic growth, and harmonised privacy protections for consumers.

Current status of data protection in MENA

Generally, the position in most of the Middle East North Africa (**MENA**) jurisdictions is that the privacy of an individual and the safeguarding of their personal data are provided under general provisions of law rather than specifically focused on the issue of "data privacy" or "data protection". There are, of course, some exceptions to this, as indicated in the report.

With the General Data Protection Regulation (GDPR), the EU is leading the charge on data privacy and protection, and the feeling in the MENA region is that it would be a positive move for nations to introduce specific, local data protection laws to follow the GDPR. A Middle East-wide data protection model law or framework would be considered to benefit both the countries and consumers at large; however, the opportunity for regional interoperability is not being leveraged at present.

Across the Gulf Cooperation Council (**GCC**) countries, jurisdictions like Bahrain and the UAE Free Zones of the DIFC and ADGM are leading the way, with robust data protection laws on the statute books. These laws are all heavily influenced by EU 1995 Data Protection Directive (**1995 Directive**), each enshrining the globally accepted fundamental principles of data protection. It therefore follows that these jurisdictions present significant opportunities for interoperability subject to the principles of lawful use, purpose limitation, data security and data minimisation. Through interoperability, those jurisdictions with mirroring data protection regimes can work together through, for example, negotiated codes of conduct that would encompass common protections together with any additional necessary, mutually agreed elements.

Saudi Arabia and the UAE are expected to soon follow Bahrain and the Free Zones. However, it is not clear whether such laws will be sector-specific or will cover all organisations, both public and private, or indeed when such laws will be put in place. Most recently, the UAE passed the Federal Law No 2 of 2019 which regulates the use of information technology and communications in the healthcare sector. This law seeks to raise the minimum bar for protection of health data and introduces certain concepts that are on a par with best international practice in data privacy law.

¹ For more information on the complex nature of data value chains, refer to the GSMA report, "The Data Value Chain", available at: https://www.gsma.com/publicpolicy/wp-content/uploads/2018/06/GSMA_Data_Value_Chain_June_2018.pdf.

Additionally, while there are regulators covering other digital issues, specific data protection authorities have not been put in place, which has created some issues around enforcement of data protection laws and awareness of the implication and interpretation of those laws. However, across those countries with specific data protection laws, there has been some momentum towards the establishment of designated, independent data protection supervisory authorities. For example, the Saudi Arabian Commission for Cybersecurity (**SACC**) recently issued a public tender to include the setting up of the SACC as the regulator for personal data protection and freedom of information.

As this report indicates, where privacy laws do exist, the principles and requirements underpinning those laws reflect those enshrined in the GDPR and its predecessor, the 1995 Directive. In some cases, those same principles are reflected in other types of laws and frameworks across the region, such as cybercrime laws. As the GSMA noted in the report *Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC can Protect Data and Drive Innovation*,² identifying commonalities and differences between privacy frameworks is a first step in building a common regional approach to privacy protection and accountable data flows.

Moving towards interoperability in MENA

The GDPR has spurred the creation and revision of privacy laws around the world, including in the MENA region. While many of these new and updated regimes draw heavily from their European counterparts, the possibility for divergence remains a risk, which can occur for a number of reasons including cultural and socio-political nuances across the different jurisdictions. Similar divergences occurred in Europe with the 1995 Directive, such as divergences in data localisation rules, registration and enforcement, and led to the birth of the GDPR which is directly applicable and almost completely harmonised across all 27 Member States.

Such divergences can often translate into differing levels of regulatory stringency which can lead to operational complications and significant cost burdens for organisations processing personal data of citizens in multiple jurisdictions. Similarly, grappling with strict data localisation requirements or other hard barriers to cross-border data transfers are likely to have a negative economic impact.

The benefit of a harmonised, sub-regional data protection framework for MENA is that it would encourage greater convergence across the region and bridge data protection gaps, enabling less restricted data flows while maintaining a similar level of data protection and reducing inconsistencies. In addition, unified regional frameworks can:

- reduce barriers to investment that restrictive data flow rules can cause;
- foster greater regional economic integration and cooperation;
- create a clearer compliance environment for businesses in which to operate; and
- help guide local-level regulations which can assist countries in better integrating with their regional neighbours.

There are of course certain barriers to achieving a regional privacy framework, particularly in terms of feasibility given the different status of data privacy laws (or lack thereof) across the region. The cost of implementation, the time needed to negotiate and achieve this and availability of the requisite skills and expertise required to manage the process must equally be considered. A regional framework must continually evolve in order to address these challenges.

In terms of how a regional framework may be achieved, a bi- or multilateral agreement based on the principle of interoperability can allow data protection authorities and other relevant government stakeholders to share knowledge, perspective, best practices, and to consider how to improve and harmonise the national data protection frameworks. Rules regarding equivalence

² GSMA report, available at: https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf

mechanisms or adequacy of protection can also encourage countries in the region to recognize similar levels of data protection offered by other countries' national laws.

European privacy law is designed to protect individuals' data and to ensure the free flow of protected, secure data across the EU, and to other countries with equivalent privacy protections. The proliferation of EU-inspired data protection laws also, in many cases, reflects the balance between the expectation of privacy and the need for commercial growth and innovation. This balance should be considered in national laws, and in the context of any regional frameworks. The key message to the MENA region is that there is a significant move towards a world where laws and regulations will regulate the ways in which organisations can responsibly use personal data. These laws should reflect the dual governmental objectives of protecting citizens, while also enabling growth and innovation, leading to a range of benefits for citizens and businesses alike.

Scope

The purpose of this report is to provide an understanding of the data privacy and protection laws and regulations that currently exist across certain jurisdictions in the MENA region. The report additionally considers these laws as they relate to other leading data privacy and protection regimes globally, specifically the GDPR. Accordingly, the objective of this report was to map the relevant laws of thirteen specific MENA jurisdictions against certain features of the GDPR. The report further sheds some light on the foundational bases for any specific data privacy and protection laws; the future of these laws in terms of updates, amendments, revisions or repeals; and any likely development(s) (if any) in this area.

Certain jurisdictions, such as Bahrain and the UAE Free Zones, have robust, European-style data privacy laws on their statute books which have been compared with the corresponding provisions in the GDPR. Other jurisdictions, such as Saudi Arabia, Jordan and Egypt, are currently in the process of drafting comprehensive laws in this area. However, as drafts of these laws have generally not been made public to date, this report does not consider these laws in any detail. In those jurisdictions with no specific data privacy and protection legislation, the report instead considers those laws containing

requirements around personal data protection and most relevant to the telecommunications sector, namely telecommunications laws and cyber security laws. While written on behalf of the GSMA, the perspective is wide and may cover several industry sectors.

The mapping exercise was limited to the following core aspects of the GDPR only:

- Cross-border data transfers;
- Data subject rights;
- Data security requirements;
- Principles of data processing;
- Data controller and data processor obligations;
- Administrative fines and regulatory sanctions; and
- Role and powers of any relevant data protection authorities.













The jurisdictions reviewed are the United Arab Emirates, the UAE Free Zones of the DIFC and ADGM, Saudi Arabia, Jordan, Kuwait, Egypt, Oman, Bahrain, Lebanon, Qatar, the Qatar Financial Centre and Turkey.

Jurisdictional overview




Jurisdiction	Overview
UAE	The UAE does not have a specific federal data protection law analogous to the GDPR, however reports suggest that a draft federal law (or laws) are in the pipeline but there is no indication of when such may be published. Telecommunications and Cyber Crime laws provide some limited data protection rights and obligations in the UAE alongside the Constitution and Penal Code. Telecoms service providers have certain Personal Data protection obligations under the Consumer Protection Regulations.
UAE Free Zones	Each of the DIFC and ADGM have enacted their own data protection laws based on international best practice, which apply to organisations in their jurisdiction. The DIFC and ADGM laws are generally consistent with data protection laws in other developed jurisdictions (specifically the 1995 Directive and the UK Data Protection Act 1998). Both have deliberately sought not to pre-empt the GDPR – rather they have adopted a "wait and see" approach before further aligning themselves with it.
Saudi Arabia	While Saudi Arabia doesn't have a specific data protection law, media reports suggest that a new freedom of information and protection of private data law is currently under review. A novel and innovative regulatory framework for cloud computing exists; one of only a few examples of cloud-specific regulatory frameworks around the world. The framework is based on the best international practice and public consultation.
Jordan	There is currently no specific data protection law in Jordan however, a draft data protection bill is currently under consultation. The draft bill appears broadly based on the GDPR, with the incorporation of the main concepts of transparency, accuracy, storage limitation and data minimisation. However, the 2018 draft is generally accepted to suffer from issues around a lack of independence of the Jordanian Privacy Commission, a failure to incorporate international standards and best practices for data protection and insufficient consideration for modern forms of data Processing.
Kuwait	There is currently no specific data protection law in Kuwait. There are limited provisions in cyber security and electronic transactions legislation however the jurisdiction lags behind other GCC nations. However, with the focus on cybersecurity, and the efforts of the Communication and Information Technology Regulatory Authority to improve the standards and practices of information security, and protect the IT infrastructure in Kuwait, it is expected that there will be developments in data protection in the near future.
Egypt	Like many other MENA jurisdictions, Egypt does not currently have a specific data protection law. A draft law regulating the freedom of data exchange and data protection is currently under discussion but has not been published. A final version of the draft is expected in 2019. The new law purports to establish a Centre for Personal Data Protection that will make and formulate various policies and regulations, and will be tasked with monitoring compliance with, and enforcing the provisions of, the new law.

Jurisdiction	Overview
Oman	Oman does not currently have a specific privacy or data protection law, but the Oman Information Technology Authority announced in 2017 that it was developing a data protection law. There is, however, no clear indication of when it will be published. It was reported that if approved and signed into law, the law will grant powerful rights to individuals in Oman, enabling them to exercise GDPR-style levels of control over their Personal Data including the ability to object to the Processing of their Personal Data and demand access to any Personal Data about them held by any organisation in Oman.
Bahrain	Bahrain was one of the first of the GCC nations to adopt its own data privacy law in 2018 which will come into force on 1 August 2019. The law aims to be consistent with international best practices and is heavily based on the GDPR. It includes the protection of individuals' privacy and specific consent requirements for data Processing, as well as the creation of a Personal Data Protection Authority. The law is directly influenced by the country's ambitious plans to become a hub for data centres.
Lebanon	Data protection is governed in Lebanon by the E-Transactions and Personal Data Law, introduced in 2004 and updated in 2018. The framework has been criticised for being weak and somewhat outdated by not reflecting the reality of online data and that the substantive provisions include vague and open-ended requirements. Additionally, experts say that the law fails to adequately protect Lebanese citizens' and residents' data by putting in place weak safeguards and only granting authority to the executive branch of the Lebanese Government. Compared with the GDPR, the law is not as detailed or comprehensive, primarily as it fails to provide for the establishment of an independent regulatory body in charge of monitoring Personal Data protection.
Qatar	Qatar was the first GCC nation to issue a generally applicable data protection law which took effect in 2017 and executive regulations further implementing it are expected to be passed in 2019. The law is modelled on and incorporates familiar concepts from other international privacy frameworks, such as the 1995 Directive (and by extension the GDPR) and mandates that any party who Processes Personal Data adhere to the principles of transparency, fairness and respect for human dignity. The Ministry of Transport and Communications is responsible for implementing and enforcing the law.
QFC	The QFC introduced its own Data Protection Regulations in 2005 and established a Data Protection Directorate responsible for implementing and enforcing the law, managing related disputes and applying GDPR standards. The regulations are largely modelled on, and inspired by, the privacy and data protection principles and guidelines contained in the 1995 Directive and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
Turkey	Turkey's Data Protection Law is predominantly modelled on the 1995 Directive, with many of the terms and central provisions very closely mirroring their equivalents in the EU law. Enactment of the Data Protection Law marks a new era for data protection in Turkey. Although the Data Protection Law is still in its infancy and no enforcement actions have yet been taken, the Personal Data Protection Board (the national supervisory authority in Turkey) has published the draft versions of secondary legislation, as well as booklets providing guidance on the implementation of the law.

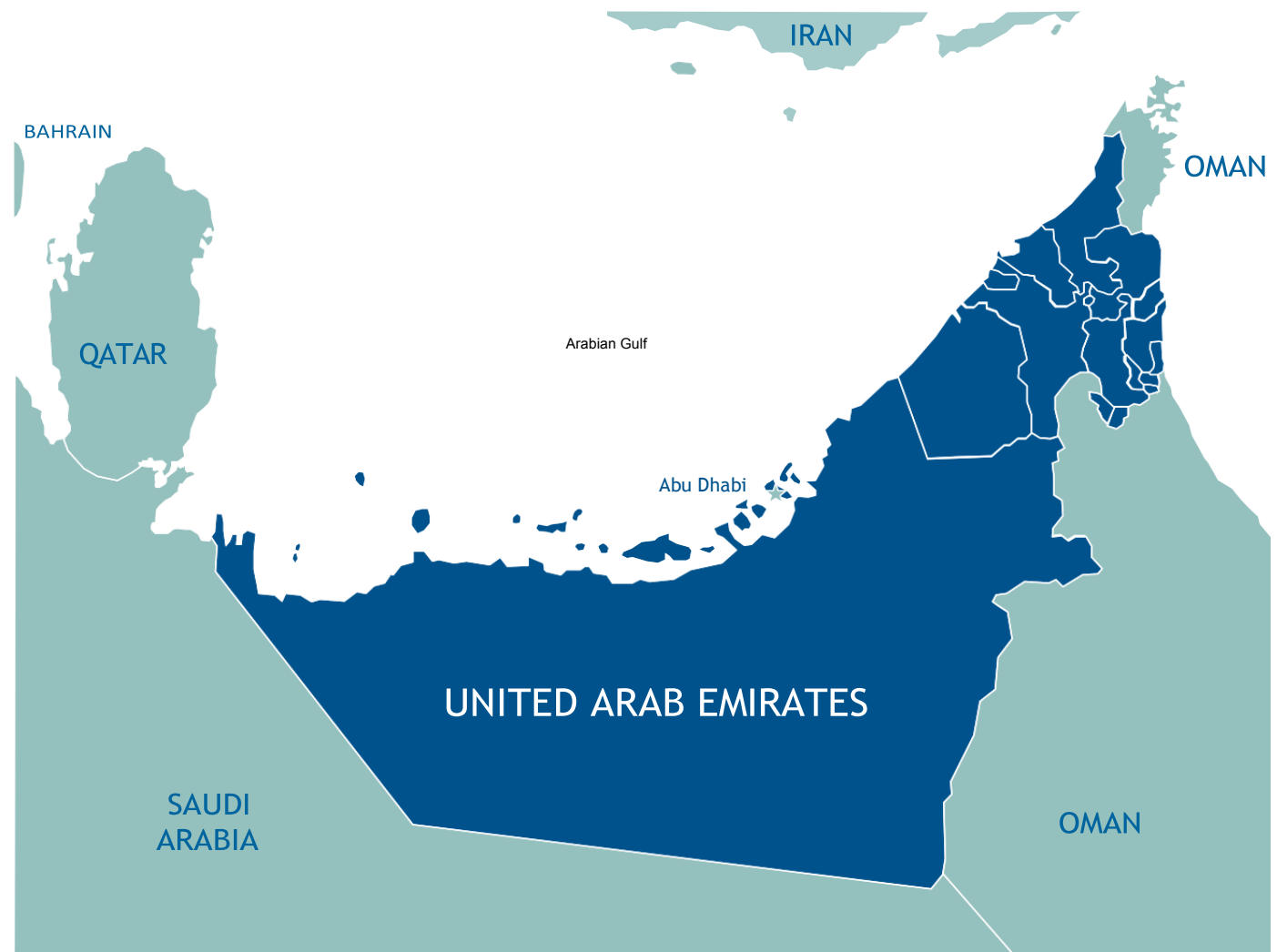
Jurisdictional GDPR alignment

Jurisdiction	GDPR alignment
UAE	
DIFC & ADGM	
Saudi Arabia	
Jordan	
Kuwait	
Egypt	
Oman	
Bahrain	
Lebanon	
Qatar	
QFC	
Turkey	

Key

-  Aligned with the GDPR
-  Partially aligned with the GDPR
-  Not aligned with the GDPR

UNITED ARAB EMIRATES (UAE)



UAE – Executive summary



The UAE does not have a comprehensive federal data protection law. However, it is understood that a draft law modelled largely on the GDPR has been circulated internally amongst certain UAE Government Departments by the Ministry of Transport and Communications. It is expected that this draft will become law by the end of 2019 / early 2020. No further information is currently available.

It is also understood that more than one federal data protection law may be published in the future, from both the financial services regulator (for all banks and financial services organisations) and the Telecommunications Regulatory Authority (TRA) (for all other public and private organisations). However, this has not been confirmed.

In addition, a draft Internet of Things Framework (IoT Framework) was reportedly circulated internally by the TRA in late 2018. Reports suggest that the IoT Framework contains provisions similar to the Saudi draft framework published in February 2019. What is known is that the IoT Framework requires any government secret, confidential or sensitive data to be stored inside the UAE and that Personal Data may be stored outside of the UAE provided that the destination country for data storage meets or exceeds any data security and user protection policies / regulations followed within the UAE.

The above notwithstanding, there are a number of laws in place that govern privacy and data security in the UAE. In addition, certain free zones including the Dubai International Financial Centre (DIFC) and the Abu Dhabi General Market (ADGM) have specific data protection laws in place. The Dubai Data Dissemination and Exchange Law (Law No 26 of 2015) also applies to the exchange of information in the Emirate of Dubai between state entities.

At federal level, the most relevant privacy law of general application is set out in the Penal Code (Federal Law 3 of 1987 as amended) and prohibits the disclosure of 'secrets' by a person entrusted with same without consent or in accordance with law. The term 'secret' is undefined, however it is generally broadly construed to cover the concepts of Personal Data, (for example, name, date of birth, sex, religion etc.).

In addition, there are several federal laws that contain provisions in relation to privacy and the protection of Personal Data including the Constitution (Federal Law No 1 of 1971), the Cyber Crime Law (Federal Law No 5 of 2012 as amended), the Telecoms Regulations (Federal Law by Decree No 3 of 2003 as amended) and the Consumer Protection Regulations passed pursuant to the Telecoms Regulations.

	GDPR	Telecoms Regulations	Cyber Crime Law	General Observations
Principles of Data Processing	<p>Lawfulness, fairness, transparency Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. (Article 5(1)(a))</p> <p>Specified purposes Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. (Article 5(1)(b))</p> <p>Data minimisation Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. (Article 5(1)(c))</p> <p>Accuracy Personal Data must be accurate and, where necessary, kept up to date. (Article 5(1)(d))</p> <p>Storage limitation Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. (Article 5(1)(e))</p> <p>Integrity and confidentiality Personal Data must be processed in a way 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. (Article 5(1)(f))</p>	<p>Lawful basis An individual's consent must be obtained in order to process their Personal Data including disclosing any documents obtained by such Processing.</p> <p>Consumer regulations <i>Consumer Protection Regulations</i>, Version 1.3 (issued by the TRA on 10 January 2017), passed pursuant to the Telecoms Regulations (Consumer Regs)</p> <p>Lawful basis Under the Consumer Regs, telecoms service providers (Licensees) may not disclose Personal Data of customers unless:</p> <ul style="list-style-type: none"> permitted by law; expressly permitted by that customer; expressly permitted by any provision in the Consumer Regs or any other aspect of the Telecoms Regulations; made in the course of the Licensee making a credit check with a reputable credit reporting agency; made in response to a lawful request by law enforcement agencies to assist in the investigation of criminal activity; made in response to a lawful request from any competent authority in relation to matters involving the public interests and/or matters of state security; or made to the TRA in accordance with the Consumer Regs. (Article 13.2, Consumer Regs) 	<p>Lawful basis An individual's consent must be obtained in order to process their Personal Data including disclosing any documents obtained by such Processing.</p>	<p>At a federal level, no specific data protection law yet exists. However, it is understood that a draft law modelled largely on the GDPR has been circulated internally amongst certain UAE Government Departments by the Ministry of Transport and Communications. It is expected that this draft will become law by the end of 2019/early 2020. No further information is currently available.</p> <p>It is also understood that more than one federal data protection law may be published in the future, from both the financial services regulator (for all banks and financial services organisations) and the TRA (for all other public and private organisations). However, this has not been confirmed.</p> <p>The TRA passed the Consumer Regs pursuant to the Telecoms Regulations that contain provisions more aligned with the GDPR than any current federal law. The regulations only apply however to the telecoms sector.</p>

GDPR	Telecoms Regulations	Cyber Crime Law	General Observations
<p>Accountability The controller shall be responsible for and be able to demonstrate compliance with all the above principles. (Article 5(2))</p> <p>Lawful bases The legal bases under which Personal Data may be processed are:</p> <ul style="list-style-type: none"> • with the freely given, specific, informed and unambiguous consent of the Data Subject; • where necessary for the performance of a contract to which the Data Subject is party; • where necessary to comply with a legal obligation to which the controller is subject; • where necessary to protect the vital interests of the Data Subject or another person; • where 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 • where necessary for the purposes of the legitimate interests of the controller or a third party. (Article 6(1)) <p>Sensitive personal data The Processing of Sensitive Personal Data is prohibited, unless the:</p> <ul style="list-style-type: none"> • Data Subject has given explicit consent. (Article 9(2)(a)) • Processing is necessary in the context of employment law, or laws relating to social security and social protection. (Article 9(2)(b)) 	<p>Consent to sharing Licensees must obtain a customer's prior consent before sharing any Personal Data with its affiliates and/or other third parties not directly involved in the provision of the telecommunications services ordered by the customer. (Article 13.5, Consumer Regs)</p> <p>Further processing Licensees who have access to customer Personal Data as a result of interconnections with another Licensee are strictly prohibited from using customer Personal Data for any purposes other than interconnection. In particular, that data may not be used for any marketing purposes or anticompetitive practices. (Article 13.6, Consumer Regs)</p> <p>Data minimisation Licensees shall not require customers to provide any personal information related to any other person that is not essential and directly related to the provision of the service ordered, unless the Licensee is required to collect such information and data under the expressed instructions of a competent authority, in the interest of public or national security. (Article 13.7, Consumer Regs)</p>		

GDPR	Telecoms Regulations	Cyber Crime Law	General Observations
	<ul style="list-style-type: none"> Processing is necessary to protect vital interests of the Data Subject (or another person). (Article 9(2)(c)) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim. (Article 9(2)(d)) Processing relates to Personal Data which are manifestly made public by the Data Subject. (Article 9(2)(e)) Processing is necessary for the establishment, exercise or defence of legal claims. (Article 9(2)(f)) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law. (Article 9(2)(g)) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional. (Article 9(2)(h)) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical 		

GDPR		Telecoms Regulations	Cyber Crime Law	General Observations
	<p>devices, on the basis of EU or Member State law. (Article 9(2)(i))</p> <ul style="list-style-type: none"> Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. (Article 9(2)(j)) 			
Data Controller and Data Processor Obligations	<p>General principles The controller is responsible for compliance with the principles listed in Article 5 (as set out above).</p> <p>The controller must have regard to 'data protection by design and by default' throughout their Processing activities. (Article 25)</p> <p>Lawful processing The controller must only process Personal Data under one of the conditions laid out in Article 6 and for special categories of Personal Data those laid out in Article 9.</p> <p>Technical & organisational measures The controller is responsible for implementing appropriate technical and organisational measures to ensure and demonstrate that its Processing activities are compliant with the requirements of the GDPR. (Article 32)</p> <p>Data subject rights The controller must demonstrate the Data Subject's consent to Processing their Personal Data. The consent must be clearly presented and easily distinguished from other matters, in an intelligible and easily accessible form. The consent must be able to be withdrawn at any time. (Article 24)</p>	<p>Lawful basis An individual's consent must be obtained in order to process their Personal Data including disclosing any documents obtained by such Processing.</p> <p>Consumer regulations</p> <p>Compliance Licensees must regularly review their contract terms of the services in order to ensure compliance with the Telecoms Regulations and any other UAE laws and regulations. This may include any requirements under any federal data protection law to provide certain rights and information to Data Subjects. (Article 5.6, Consumer Regs)</p> <p>Security Licensees must take all reasonable and appropriate measures to prevent the unauthorised disclosure or the unauthorised use of customer Personal Data. (Article 13.1, Consumer Regs)</p> <p>Licensees shall take all reasonable measures to protect the privacy of customer Personal Data that it maintains in its files, whether in electronic or paper form. Licensees shall use reliable security measures against risks such as loss or unauthorised access, destruction, leakage, inappropriate use, modification</p>	<p>Lawful basis An individual's consent must be obtained in order to process their Personal Data including disclosing any documents obtained by such Processing.</p>	<p>The GDPR places significantly more onerous burdens on Data Controllers and Data Processors than any law in the UAE.</p> <p>Data Processing agreements are not governed by any laws or regulations in the UAE. No standard form or precedent data Processing agreements have been approved by the national authorities or UAE courts.</p> <p>The TRA passed the Consumer Regs pursuant to the Telecoms Regulations and contain provisions much more aligned with the GDPR than any current federal law. The regulations only apply however to the telecoms sector.</p>

GDPR	Telecoms Regulations	Cyber Crime Law	General Observations
<p>The controller must make reasonable efforts to verify parental consent (when the child is under 16, although in some Member States may be as young as 13).</p> <p>Choosing a data processor The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of this Regulation and ensure the protection of the rights of the Data Subject.</p> <p>Processing by a processor shall be governed by a contract or other legal act recognised under EU law. (Article 28)</p> <p>Notifications In the case of a Personal Data breach, the controller must notify the DPSC of the breach. This must be done without due delay and, where feasible, not later than 72 hours after having become aware of it. (Article 33)</p> <p>Record keeping Each controller must maintain a record of its Processing activities. (Article 30)</p> <p>Appoint a representative The controller must appoint an EU representative in certain situations. (Article 27)</p> <p>Appoint a DPO The controller must appoint a Data Protection Officer (DPO) in certain situations. (Article 37(1))</p>	<p>and/or unauthorised disclosure. (Article 13.3, Consumer Regs)</p> <p>Note: There is no definition of 'reasonable and appropriate measures'.</p> <p>Access by personnel Licensees shall limit access to customer Personal Data to its trained and authorised personnel who will include the Licensee's employees, directors, independent contractors and consultants, who are bound to protect the Licensees confidential information (which includes customer Personal Data) from unauthorised use and disclosure under the terms of a written agreement. Licensees shall ensure that personnel engaged in the handling of customer Personal Data are fully aware of, and adequately trained in the Licensee's security and privacy protection practices. (Article 13.4, Consumer Regs)</p> <p>Choosing a data processor Where it is necessary to provide customer Personal Data to affiliates or other third parties who are directly involved in the supply of the telecommunications services ordered by customers, the third-parties are required to take all reasonable and appropriate measures to protect the confidentiality and security of the customer Personal Data and to use it only as required for the purposes of providing the telecommunication service. Licensees shall ensure that the contract between them and any affiliate or other third party holds that third party responsible for the privacy and protection of the customer Personal Data. (Article 13.8, Consumer Regs)</p>		

GDPR		Telecoms Regulations	Cyber Crime Law	General Observations
Data Subject Rights	<p>Transparent communication In order to ensure that Personal Data are processed fairly and lawfully, controllers must provide certain minimum information to Data Subjects, regarding the collection and further Processing of their Personal Data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. (Articles 5(1)(a), 12-14)</p>	No specific relevant provisions exist.	No specific relevant provisions exist.	There are very limited measures in place under UAE law to enable Data Subjects to vindicate their rights with no general protection of Data Subject rights in line with the GDPR.
	<p>Data subject rights Data controllers have a legal obligation to give effect to the rights of Data Subjects. (Article 12(2))</p>	<p><u>Consumer regulations</u></p>		
	<p>Identifying data subjects Data controllers must not refuse to give effect to the rights of a Data Subject unless the controller cannot identify the Data Subject. The controller must use all reasonable efforts to verify the identity of Data Subjects. Where the controller has reasonable doubts as to the identity of the Data Subject, the controller may request the provision of additional information necessary to confirm the identity of the Data Subject, but is not required to do so. (Article 12(2), (6))</p>	<p>Right of access Where a customer requests the Licensee to disclose his or her own Personal Data to that customer, the Licensee shall disclose it free of charge and without delay after an adequate verification process. (Article 13.9, Consumer Regs)</p>		
	<p>Time limits A controller must, within one month of receiving a request made under those rights, provide any requested information in relation to any of the rights of Data Subjects. If the controller fails to meet this deadline, the Data Subject may complain to the relevant DPSA and may seek a judicial remedy. Where a controller receives large numbers of requests, or especially complex requests, the timelimit</p>			

GDPR	Telecoms Regulations	Cyber Crime Law	General Observations
<p>may be extended by a maximum of two further months. (Article 12(3) - (4))</p> <p>Basic information Data Subjects have the right to be provided with information on the identity of the controller, the reasons for Processing their Personal Data and other relevant information necessary to ensure the fair and transparent Processing of Personal Data. (Articles 13 and 14)</p> <p>Right of access Data Subjects have the right to obtain:</p> <ul style="list-style-type: none"> • confirmation of whether, and where, the controller is Processing their Personal Data; • information about the purposes of the Processing; • information about the categories of data being processed; • information about the categories of recipients with whom the data may be shared; • information about the period for which the data will be stored (or the criteria used to determine that period); • information about the existence of the rights to erasure, to rectification, to restriction of Processing and to object to Processing; • information about the existence of the right to complain to the DPSA; • where the data were not collected from the Data Subject, information as to the source of the data; and • information about the existence of, and an explanation of the logic involved in any automated Processing that has a significant effect on Data Subjects; and 			

GDPR	Telecoms Regulations	Cyber Crime Law	General Observations
<ul style="list-style-type: none"> Data Subjects may request a copy of the Personal Data being processed. (Article 15) <p>Access fees Data controllers must give effect to the rights of access, rectification, erasure and the right to object, free of charge. The controller may charge a reasonable fee for "repetitive requests", "manifestly unfounded or excessive requests" or "further copies". (Articles 12(5), 15(3), (4))</p> <p>Rectification Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data Subjects have the right to rectification of inaccurate Personal Data. (Articles 5(1)(d), 16)</p> <p>Erasure Data Subjects have the right to erasure of Personal Data if:</p> <ul style="list-style-type: none"> the data are no longer needed for their original purpose (and no new lawful purpose exists); the lawful basis for the Processing is the Data Subject's consent, the Data Subject withdraws that consent, and no other lawful ground exists; the Data Subject exercises the right to object, and the controller has no overriding grounds for continuing the Processing; the data have been processed unlawfully; or erasure is necessary for compliance with EU law or the national law of the relevant Member State. (Article 17) 			

GDPR	Telecoms Regulations	Cyber Crime Law	General Observations
	<p>Restrict processing Data Subjects have the right to restrict the Processing of Personal Data (meaning that the data may only be held by the controller, and may only be used for limited purposes) if:</p> <ul style="list-style-type: none"> • the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); • the Processing is unlawful and the Data Subject requests restriction (as opposed to exercising the right to erasure); • the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or • if verification of overriding grounds is pending, in the context of an erasure request. (Article 18) <p>Portability Data Subjects have a right to:</p> <ul style="list-style-type: none"> • receive a copy of their Personal Data in a structured, commonly used, machine-readable format that supports re-use; • transfer their Personal Data from one controller to another; • store their Personal Data for further personal use on a private device; and • have their Personal Data transmitted directly between controllers without hindrance. (Article 20) 		

GDPR	Telecoms Regulations	Cyber Crime Law	General Observations
<p>Object to processing Data Subjects have the right to object, on grounds relating to their particular situation, to the Processing of Personal Data, where the basis for that Processing is either:</p> <ul style="list-style-type: none"> • public interest; or • legitimate interests of the controller. <p>The controller must cease such Processing unless the controller:</p> <ul style="list-style-type: none"> • demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject; or • requires the data in order to establish, exercise or defend legal rights. (Article 21) <p>Where Personal Data are processed for scientific and historical research purposes or statistical purposes, the Data Subject has the right to object, unless the Processing is necessary for the performance of a task carried out for reasons of public interest. (Articles 21(6), 83(1))</p> <p>Object to direct marketing Data Subjects have the right to object to the Processing of Personal Data for the purpose of direct marketing, including profiling. (Article 21(2) – (3))</p> <p>Duty to inform of right to object The right to object to Processing of Personal Data noted above must be communicated to the Data Subject no later</p>			

GDPR		Telecoms Regulations	Cyber Crime Law	General Observations
	<p>than the time of the first communication with the Data Subject.</p> <p>This information should be provided clearly and separately from any other information provided to the Data Subject. (Articles 3(2)(b), 14(2)(c), 15(1)(e), 21(4))</p> <p>Automated processing Data Subjects have the right not to be subject to a decision based solely on automated Processing which significantly affect them (including profiling). Such Processing is permitted where:</p> <ul style="list-style-type: none"> • it is necessary for entering into or performing a contract with the Data Subject provided that appropriate safeguards are in place; • it is authorised by law; or • the Data Subject has explicitly consented and appropriate safeguards are in place. (Article 22) 			
Cross-Border Transfer Rules	<p>General prohibition Cross-border personal data transfers may only take place if the transfer is made to an Adequate Jurisdiction or the data exporter has implemented a lawful data transfer mechanism (or an exemption or derogation applies). (Articles 44, 45)</p> <p>Adequacy decisions Cross-border data transfers may take place if the third country receives an Adequacy Decision from the EU Commission. (Articles 44, 45)</p> <p>The EU Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey,</p>	No specific relevant provisions exist.	No specific relevant provisions exist.	<p>There is no regulation currently dealing specifically with the transfer of Personal Data outside the UAE. Data transfer agreements are not governed by any laws or regulations in the UAE. No standard form or precedent data transfer agreements have been approved by the national authorities or UAE courts.</p> <p>NOTE: Under the GDPR, Cross-border data transfers may take place on the basis of standard data protection clauses approved by the EU Commission ("Model Clauses"). The current set of Model Clauses are currently being challenged as a form of</p>

GDPR	Telecoms Regulations	Cyber Crime Law	General Observations
<p>Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the USA (subject to compliance with the terms of the US-EU Privacy Shield).</p> <p>Public authorities Cross-border data transfers between public authorities may take place under agreements between public authorities, which do not require any specific authorisation from a DPSA. (Articles 46(2)(a), 46(3)(b))</p> <p>Binding Corporate Rules Cross-border data transfers within a corporate group may take place on the basis of Binding Corporate Rules ("BCRs"). BCRs require approval from DPSAs, but approved, individual transfers made under the BCRs do not require further approval. (Articles 4(20) 46(2)(b), 47)</p> <p>Model clauses Cross-border data transfers may take place on the basis of the Model Clauses entered into between the data exporter and data recipient. Existing Model Clauses implemented under the 1995 Directive remain valid until amended, replaced or repealed under the GDPR. (Articles 28(6)-(8), 46(2)(c), 57(1)(j), (r), 93(2))</p> <p>Other mechanisms Cross-border data transfers may take place on the basis, <i>inter alia</i>, of:</p> <ul style="list-style-type: none"> • standard data protection clauses adopted by one or more DPSAs under the GDPR. (Articles 46(2)(d), 64(1)(d), 57(1)(j), (r), 93(2)) • an approved code of conduct, together with binding and enforceable 			<p>appropriate data transfer mechanism; therefore their future is uncertain.</p> <p>In January 2019, the Irish Supreme Court (as part of the <i>Schrems v Facebook</i> litigation) heard an appeal by Facebook over a decision of the Irish High Court to refer a number of questions to the Court of Justice of the EU ("CJEU") regarding the validity of this data transfer mechanism. The Supreme Court will publish its decision in due course. If Facebook is unsuccessful in its appeal, the CJEU will rule on these questions, which may result in a declaration that the Model Clauses are no longer valid as a transfer mechanism.</p>

GDPR	Telecoms Regulations	Cyber Crime Law	General Observations
	<p>commitments to provide appropriate safeguards. (Articles 40, 41, 46(2)(e))</p> <ul style="list-style-type: none"> • certifications together with binding and enforceable commitments of the data importer to apply the certification to the transferred data. (Articles 42, 43, 46(2)(f)) • ad hoc clauses conforming to the GDPR and approved by the relevant DPSA. (Articles 46(3)(a), (4), 63)) • administrative arrangements between public authorities (e.g., MOUs) subject to DPSA approval. (Articles 46(3)(b), (4), 63) <p>Derogations Cross-border data transfers may be made on the basis, <i>inter alia</i>, that:</p> <ul style="list-style-type: none"> • the Data Subject explicitly consents having been informed of the possible risks of such transfer. (Article 49(1)(a), (3)) • the performance of a contract between the Data Subject and the controller. (Article 49(1)(b), (3)) • it is necessary for the purposes of performing or concluding a contract in the interests of the Data Subject. (Article 49(1)(c), (3)) • the transfer is necessary for important reasons of public interest. (Article 49(1)(d), (4)) • it is necessary for the purposes of legal proceedings, or obtaining legal advice. (Article 49(1)(e)) • the transfer is necessary in order to protect the vital interests of the Data Subject, where the Data Subject is incapable of giving consent. (Article 49(1)(f)) • the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by those of 		

GDPR		Telecoms Regulations	Cyber Crime Law	General Observations
	the individual subject to informing the relevant DP/SA and the Data Subjects. (Article 49(1), (3), (6))			
Personal Data Security	<p>Security Data controllers must implement appropriate technical and organisational security measures to protect Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.</p> <p>Depending on the nature of the Processing, these measures may include:</p> <ul style="list-style-type: none"> • encryption of the Personal Data; • on-going reviews of security measures; • redundancy and back-up facilities; and • regular security testing. (Article 32) 	<p>No specific relevant provisions exist.</p> <p>Consumer regulations</p> <p>Security Licensees must take all reasonable and appropriate measures to prevent the unauthorised disclosure or the unauthorised use of customer Personal Data. (Article 13.1, Consumer Regs)</p> <p>Licensees shall take all reasonable measures to protect the privacy of customer Personal Data that it maintains in its files, whether in electronic or paper form. Licensees shall use reliable security measures against risks such as loss or unauthorised access, destruction, leakage, inappropriate use, modification and/or unauthorised disclosure. (Article 13.3, Consumer Regs)</p> <p>Third parties Where a Licensee shares customer Personal Data with an affiliate or other third party, those the third-parties are required to take all reasonable and appropriate measures to protect the confidentiality and security of the customer Personal Data and to use it only as required for the purposes of providing the telecommunication service. (Article 13.8, Consumer Regs)</p>	No specific relevant provisions exist.	There are no specific provisions relating to Personal Data security akin to the GDPR outside the requirement to take reasonable and appropriate measures to protect the Personal Data and information against loss, damage, disclosure, replacement with incorrect data or information, or addition of untrue information thereto under the Consumer Regs. These regulations provide no guidance on what may be included in "appropriate measures".
Administrative Fines and Regulatory Sanctions	<p>Judicial remedies Data Subjects have the right to an effective judicial remedy against:</p>	<p>Penalties Anyone who:</p>	<p>Medical data Anyone who obtains, acquires, amends, damages or discloses without permission the statements of any Electronic</p>	The absence of a national data protection supervisory authority means that there is no effective supervision and/or enforcement of Data Subject

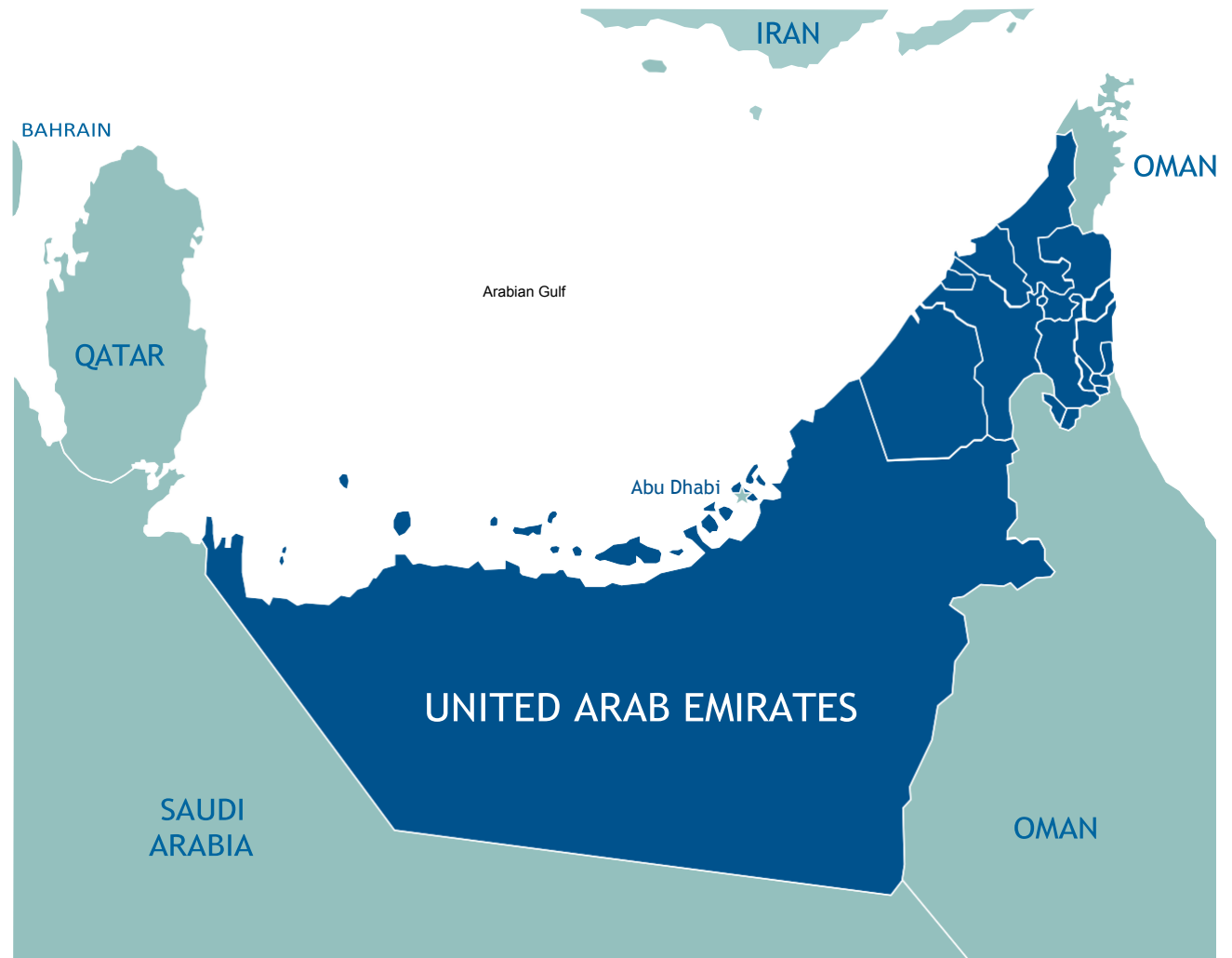
GDPR	Telecoms Regulations	Cyber Crime Law	General Observations
<ul style="list-style-type: none"> • decisions of a DPSCA concerning them; • any failure by a DPSCA to deal with, or respond to, a complaint within three months; and • any unlawful Processing of their Personal Data by a controller or processor. (Article 78-79) <p>Compensation & liability A Data Subject who has suffered harm as a result of the unlawful Processing of his or her Personal Data has the right to receive compensation from the controller or processor for the harm suffered:</p> <ul style="list-style-type: none"> • Any controller involved in the Processing is liable for the harm caused. • A processor is liable for the harm caused by any of its (or its sub-processor's) Processing activities that are not in compliance with its obligations under the GDPR, or are in breach of the controller's instructions. • To ensure effective compensation, each controller or processor will be held liable for the entirety of the harm caused, if they are involved in the same Processing and responsible for that harm. (Article 82(1)-(2), (4)) <p>Joint-controller liability Data Subjects are entitled to enforce their rights against any of the joint controllers. Each joint controller is liable for the entirety of the damage, although national law may apportion liability between them. If one joint controller has paid full compensation, it may then bring proceedings against the other joint controllers to recover their</p>	<ul style="list-style-type: none"> • illegally copies, discloses, or distributes the content of a telephone call or message relayed through a public telecommunications network; or • eavesdrops on telephone conversations without prior authorisation from the relevant judicial authorities, <p>shall be subject to:</p> <ul style="list-style-type: none"> • imprisonment for not less than 1 year; and/or • a fine between AED50,000 - AED200,000. (Article 72) 	<p>Document or Electronic Information through an Information Network, Electronic Site, Electronic Information System or an Information Technology Tool and these statements or Information relate to medical examinations or a medical diagnoses or treatment or medical care or records shall be subject to temporary imprisonment. (Article 7)</p> <p>Bank account & credit cards Anyone who unlawfully reaches by using the Information Network or Electronic Information System or any of the Information Technology Tool to the numbers or statements or a credit or electronic card or statements of bank accounts or any means of electronic payment shall be subject to:</p> <ul style="list-style-type: none"> • imprisonment between 6 months and 1 year; and/ or • a fine between AED100,000 – 1,000,000 (Article 12) <p>Intercepting communications Anyone who intentionally and without permission captures or intercepts any communication (including emails) through any Information Network and discloses it shall be subject to:</p> <ul style="list-style-type: none"> • imprisonment for not less than 1 year; and/or • a fine between AED150,000 - 500,000. (Article 15) <p>Invasion of privacy Any person who uses an Information Network, Electronic Information System or any of the Information Technology Tools in</p>	<p>rights or data protection principles in the UAE.</p> <p>Cybercrime is severely punished under the Cyber Crimes Law and penalties are imposed for invasion of privacy, disclosure of confidential information, electronic piracy, email theft and other unlawful activities.</p>

GDPR	Telecoms Regulations	Cyber Crime Law	General Observations
<p>portions of the damages. (Article 26(3), 82(3)-(5))</p> <p>Exemptions from liability A controller or processor is exempt from liability if it proves that it is not responsible for the event giving rise to the harm. There is no mention of force majeure events. (Article 82(3))</p> <p>Administrative fines The maximum fine that can be imposed for serious infringements of the GDPR is the greater of €20 million or 4% of an undertaking's worldwide turnover for the preceding financial year. (Article 83(5) – (6))</p> <p>Fine criteria When deciding whether to impose a fine and deciding on the amount, DPSAs are required to give due regard to a range of issues, including:</p> <ul style="list-style-type: none"> • the nature, gravity and duration of the infringement; • the number of Data Subjects affected and the level of harm suffered by them; • the intentional or negligent character of the infringement; • any action taken by the controller or processor to mitigate the harm; • any relevant previous infringements by the controller or processor; • the degree of co-operation with the relevant DPSA; • whether the infringement was self-reported by the controller or processor; and • any other aggravating or mitigating factors. (Article 82(3)) 		<p>assaulting the privacy of a person in cases other than those permitted in Law shall be subject to:</p> <ul style="list-style-type: none"> • imprisonment for not less than six months and/or • a fine between AED150,000 – 500,000. (Article 21) <p>Invasions of privacy can occur by:</p> <ul style="list-style-type: none"> • overhearing, interception, recording, transferring, transmitting or disclosure of conversations, communications or audio or visual materials; • capturing pictures of third party or preparing electronic pictures or transferring, exposing, copying or keeping those pictures; • publishing electronic news or pictures or photographs, scenes, comments, statements or information even if they were correct and real. <p>Confidential information Anyone who uses without permission any Information Network, Electronic Site or Information Technology Tool to expose Confidential Information obtained by occasion or because of his work shall be subject to:</p> <ul style="list-style-type: none"> • imprisonment not less than 6 months; and/or • a fine between AED500,000 – 1,000,000. (Article 22) <p>Note: 'Confidential Information' means any information or data the third party are not allowed to view or disclose except with</p>	

GDPR		Telecoms Regulations	Cyber Crime Law	General Observations
			a prior permission from the concerned owner.	
Role and Powers of any relevant Data Protection Supervisory Authority	<p>Independence DPSAs must act independently and operate free from all outside influences, including government control. (Article 52)</p> <p>Tasks The tasks of DPSAs include obligations to:</p> <ul style="list-style-type: none"> monitor and enforce the application of the GDPR; promote awareness of the risks, rules, safeguards and rights pertaining to Personal Data (especially in relation to children); advise national and governmental institutions on the application of the GDPR; hear claims brought by Data Subjects or their representatives, and inform Data Subjects of the outcome of such claims; establish requirements for Impact Assessments; encourage the creation of Codes of Conduct and review certifications; authorise Model Clauses and BCRs; keep records of sanctions and enforcement actions; and fulfil "any other tasks related to protection of Personal Data". (Article 55, 57) <p>Powers DPSAs are empowered to oversee enforcement of the GDPR, investigate breaches of the GDPR and bring legal proceedings where necessary. (Article 58)</p>	<p>The TRA oversees the telecommunications sector in the UAE and enforces the Telecoms Law and Consumer Regs.</p> <p>Confiscation orders A confiscation order will be issued for any wire or wireless equipment or other devices or hardware used in a manner contrary to the law, its implementing regulations or the regulations, decisions, instructions and rules issued pursuant thereto. The courts may further order that the equipment, hardware and devices be destroyed if necessary. (Article 76)</p> <p>Consumer regulations</p> <p>Provide information The TRA may request any Licensee to provide the TRA with any customer Personal Data that is essential to enable the TRA to fulfil its duties. Any such request shall be made in writing and the Licensee to which the request is addressed shall take all reasonable measures to supply the requested customer Personal Data as directed by the TRA. (Article 13.10, Consumer Regs)</p> <p>Attendance at premises The TRA may, upon serving reasonable notice to a Licensee, visit the premises of a Licensee or its affiliate(s) where customer Personal Data is stored by that Licensee or its affiliate(s) in order that the TRA can review the security measures taken by the Licensee or its affiliate(s) with</p>	<p>The National E-Security Authority regulates the protection of communications networks and information systems in the UAE.</p> <p>The Cyber Crimes Law is enforced by the UAE courts.</p>	<p>The absence of a national data protection supervisory authority means that there is no effective supervision and/or enforcement of Data Subject rights or data protection principles in the UAE.</p>

GDPR	Telecoms Regulations	Cyber Crime Law	General Observations
		<p>respect to maintaining the security of that Subscriber Information. (Article 13.11, Consumer Regs)</p> <p>Removal of personal data</p> <p>In the event that the TRA, acting reasonably, is not satisfied with the security arrangements at a particular premises, the TRA reserves the right to instruct the Licensee, or instruct the Licensee to instruct its affiliate(s), to strengthen the security arrangements at that particular premises or relocate the storage of customer Personal Data to a more secure premises as may be deemed appropriate, and justified, by the TRA.</p> <p>(Article 13.11, Consumer Regs)</p>	

UAE Free Zones (DIFC & ADGM)



UAE Free Zones – Executive summary



Although the UAE does not have a comprehensive data protection law at federal level, certain free zones including the Dubai International Financial Centre (**DIFC**) and the Abu Dhabi General Market (**ADGM**) do have specific data protection laws in place.

The DIFC implemented the *DIFC Data Protection Law* (DIFC Law No 1 of 2007) as amended by the *Data Protection Law Amendment Law* (DIFC Law No 5 of 2012) (**Data Protection Laws**). In addition, the Commissioner of Data Protection (**CDP**) has issued the *Data Protection Regulations* (together with the Data Protection Laws, the **DIFC Laws**). The DIFC Laws apply in the jurisdiction of the DIFC and are therefore applicable to all DIFC entities, both regulated and non-regulated by the DIFC Financial Services Authority.

The ADGM has also implemented comprehensive data protection legislation in the *ADGM Data Protection Regulations 2015* as amended by the *Data Protection (Amendment) Regulation 2018* (**ADGM Laws**). The Office of Data

Protection is the independent data protection regulator for the ADGM and is based within the ADGM Registration Authority. The ADGM Laws apply in the jurisdiction of the ADGM and are therefore applicable to all ADGM entities, both regulated and non-regulated by the ADGM Financial Services Regulatory Authority.

The DIFC Laws and ADGM Laws are largely modelled on, and inspired by, the privacy and data protection principles and guidelines contained in the 1995 Directive and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Interestingly, whilst EU laws continue to be a model for general guidance to the Free Zones in the administration of their respective data protection laws, both have deliberately sought not to pre-empt the GDPR – particularly the ADGM in its 2018 amending regulations. Instead, both regulators have chosen to adopt a "wait and see" approach on the new EU legislation before deciding whether their own laws will be further amended to align with the GDPR.

	GDPR	DIFC Laws	ADGM Laws	General Observations
Principles of Data Processing	<p>Lawfulness, fairness, transparency Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. (Article 5(1)(a))</p>	<p>Fairly, lawfully and securely Data Controllers must ensure that Personal Data are processed fairly, lawfully and securely. (Article 8(1)(a))</p>	<p>Fairly, lawfully and securely Data controllers shall ensure that Personal Data which they process are processed fairly, lawfully and securely. (Article 1(1)(a))</p>	<p>Status Both the DIFC and the ADGM have specific data protection laws that apply to the Processing of Personal Data in each of these Free Zones respectively.</p>
	<p>Specified purposes Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. (Article 5(1)(b))</p>	<p>Specified purposes Personal Data must be processed for specified, explicit and legitimate purposes in accordance with the Data Subject's rights and not further processed in a way incompatible with those purposes or rights. (Article 8(1)(b))</p>	<p>Specified purposes Personal Data must be processed for specified, explicit and legitimate purposes in accordance with Data Subjects rights and not further processed in ways incompatible with those purposes and rights. (Article 1(1)(b))</p>	<p>Basis Both the DIFC Laws and the ADGM Laws are broadly consistent with the 1995 Directive and therefore by extension, the GDPR.</p>
	<p>Data minimisation Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. (Article 5(1)(c))</p>	<p>Data minimisation Personal Data must be adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed. (Article 8(1)(c))</p>	<p>Data minimisation The Personal Data must be adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed. (Article 1(1)(c))</p>	<p>Looking forward At a federal level, no specific statutory data protection law yet exists. However, it is understood that a draft law modelled largely on the GDPR has been circulated internally amongst certain UAE Government Departments by the Ministry of Transport and Communications. It is expected that this draft will become law by the end of 2019. No further information is currently available.</p>
	<p>Accuracy Personal Data must be accurate and, where necessary, kept up to date. (Article 5(1)(d))</p>	<p>Storage limitation Personal Data must be 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. (Article 8(1)(e))</p>	<p>Storage limitation Personal Data must be accurate and, where necessary, kept up to date.</p>	<p>It is understood that more than one federal data protection law may be published in the future, from both the financial services regulator (for all banks and financial services organisations) and the Telecommunications Regulatory Authority (for all other public and private organisations). However, this has not been confirmed.</p>
	<p>Storage limitation Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. (Article 5(1)(e))</p>	<p>Accuracy Data controllers must ensure Personal Data is accurate and, where necessary, kept up to date. (Article 8(1)(d))</p>	<p>Accuracy Every reasonable step shall be taken by controllers to ensure that Personal Data which are accurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. (Article 1(2))</p>	
	<p>Integrity and confidentiality Personal Data must be processed in a way 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. (Article 5(1)(f))</p>	<p>Data controllers must take every reasonable step to ensure that inaccurate or incomplete Personal Data, having regard to the purposes for which it was collected or further processed, is erased or rectified. (Article 8(2))</p>		

GDPR		DIFC Laws	ADGM Laws	General Observations
	<p>Accountability The controller shall be responsible for and be able to demonstrate compliance with all the above principles. (Article 5(2))</p> <p>Lawful bases The legal bases under which Personal Data may be processed are</p> <ul style="list-style-type: none"> • with the freely given, specific, informed and unambiguous consent of the Data Subject; • where necessary for the performance of a contract to which the Data Subject is party; • where necessary to comply with a legal obligation to which the controller is subject; • where necessary to protect the vital interests of the Data Subject or another person; • where 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 • where necessary for the purposes of the legitimate interests of the controller or a third party. (Article 6(1)) 			
Data Controller and Data Processor Obligations	<p>General principles The controller is responsible for compliance with the principles listed in Article 5 (as set out above).</p> <p>The controller must have regard to 'data protection by design and by default' throughout their Processing activities. (Article 25)</p>	<p>General principles The controller is responsible for compliance with the principles listed in article 8 (as set out above).</p> <p>Legitimate processing The controller must comply with the requirements for legitimate Processing.</p> <p>Personal Data may only be processed if:</p>	<p>General principles The controller is responsible for compliance with the principles listed in Article 1 (as set out above).</p> <p>Legitimate processing The controller must comply with the requirements for the legitimate Processing of Personal Data: Personal Data may only be processed if:</p>	Both the DIFC and ADGM, being based on the 1995 Directive, largely mirror the GDPR in terms of obligations imposed on Data Controllers and Data Processors.

GDPR	DIFC Laws	ADGM Laws	General Observations
	<p>Lawful processing The controller must only process Personal Data under one of the conditions laid out in Article 6 and for special categories of Personal Data those laid out in Article 9.</p> <p>Sensitive personal data The Processing of sensitive Personal Data is prohibited, unless the:</p> <ul style="list-style-type: none"> • Data Subject has given explicit consent. (Article 9(2)(a)) • Processing is necessary in the context of employment law, or laws relating to social security and social protection. (Article 9(2)(b)) • Processing is necessary to protect vital interests of the Data Subject (or another person). (Article 9(2)(c)) • Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim. (Article 9(2)(d)) • Processing relates to Personal Data which are manifestly made public by the Data Subject. (Article 9(2)(e)) • Processing is necessary for the establishment, exercise or defence of legal claims. (Article 9(2)(f)) • Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law. (Article 9(2)(g)) • Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity 	<ul style="list-style-type: none"> • The Data Subject has given his written consent to the Processing (Article 9 (a)) • 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. (Article 9(b)) • Processing is necessary for compliance with any legal obligation. (Article 9(c)) • 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 DSFA, 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. (Article 9(d)) • Processing is necessary for the purposes of the legitimate interests of the controller or by the third party to whom the Personal Data is disclosed, except where such interests are overridden by compelling legitimate interests of the Data Subject. (Article 9(e)) <p>Sensitive personal data Sensitive Personal Data shall not be processed unless:</p> <ul style="list-style-type: none"> • Data Subject has given his written consent to the Processing. (Article 10(1)(a)) • Processing is necessary for the purposes of carrying out the obligations and specific rights of the controller (Article 10(1)(b)) 	<ul style="list-style-type: none"> • The Data Subject has given his written consent; (Article 2(a)) • 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. (Article 2(b)) • Processing is necessary for compliance with any legal or regulatory obligation. (Article 2(c)) • Processing necessary to protect vital interests of Data Subject (Article 2(d)) • Processing is necessary for the performance of a task carried out in the interests of the ADGM or in the exercise of the Board's, the Court's, the Registrar's or the Regulator's functions or powers vested in the Data Controller or in a third party to whom the Personal Data are disclosed (Article 2(e)) • Processing is necessary for the purposes of the legitimate interests of the controller or by the third party to whom the Personal Data is disclosed, except where such interests are overridden by compelling legitimate interests of the Data Subject. (Article 2(f)) <p>Sensitive personal data Sensitive Personal Data may only be processed if:</p> <ul style="list-style-type: none"> • Data Subject has given his written consent to the Processing. (Article 3 (1)(a)) • Processing is necessary for the purposes of carrying out the

GDPR	DIFC Laws	ADGM Laws	General Observations
<p>of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional. (Article 9(2)(h))</p> <ul style="list-style-type: none"> Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law. (Article 9(2)(i)) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. (Article 9(2)(j)) <p>Technical & organisational measures The controller is responsible for implementing appropriate technical and organisational measures to ensure and demonstrate that its Processing activities are compliant with the requirements of the GDPR. (Article 32)</p> <p>Data subject rights The controller must demonstrate the Data Subject's consent to Processing their Personal Data. The consent must be clearly presented and easily distinguished from other matters, in an intelligible and easily accessible form. The consent must be able to be withdrawn at any time. (Article 24)</p>	<ul style="list-style-type: none"> Processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is incapable of giving consent. (Article 10(1)(c)) Processing carried out in the course of legitimate activities with appropriate guarantees by a foundation, association or any other non-profit seeking body if Processing relates solely to members of the body or to persons who have a regular connection with it and that the Personal Data is not disclosed to a third party without the Data Subjects consent. (Article 10(1)(d)) Processing relates to Personal Data that has been manifestly made public by the Data Subject or is necessary for legal claims. (Article 10(1)(e)) Processing necessary for compliance with regulatory or legal obligation to which controller is subject. (Article 10(1)(f)) Processing necessary to uphold legitimate interests of controller recognised in the international financial markets (Article 10(1)(g)) Processing necessary to comply with regulatory or professional requirements (Article 10(1)(h)) Processing required for preventative medicine and the like. (Article 10(1)(i)) Processing required to protect the public against financial loss, dishonesty, etc. (Article 10(1)(j)) Authorised in writing by the Commissioner of Data Protection (Article 10(1)(k)) 	<p>obligations and specific rights of the controller (Article 3(1)(b))</p> <ul style="list-style-type: none"> Processing is necessary to protect the vital interests of the Data Subject or of another person where Data Subject is incapable of giving consent. (Article 3(1)(c)) Processing carried out in the course of legitimate activities with appropriate guarantees by a foundation, association or any other non-profit seeking body if Processing relates solely to members of the body or to persons who have regular connection with it and that the Personal Data is not disclosed to a third party without the Data Subjects consent. (Article 3(1)(d)) Processing relates to Personal Data that has been manifestly made public by the Data Subject or is necessary for legal claims (Article 3(1)(e)) Processing necessary to comply with regulatory or legal obligations to which the controller is subject. (Article 3(1)(f)) Processing necessary to uphold legitimate interests of controller recognised in the international financial markets. (Article 3(1)(f)) Processing necessary to comply with regulatory or professional requirements (Article 3(1)(h)) Processing required for preventative medicine and the like. (Article 3(1)(i)) <p>The controller must comply with the requirements in Articles 4 and 5 when transferring Personal Data out of the ADGM. (See below in Cross-Border Transfer section).</p>	

GDPR	DIFC Laws	ADGM Laws	General Observations
<p>The controller must make reasonable efforts to verify parental consent (when the child is under 16, although in some member states may be as young as 13).</p> <p>Choosing a data processor The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of this Regulation and ensure the protection of the rights of the Data Subject.</p> <p>Processing by a processor shall be governed by a contract or other legal act. (Article 28)</p> <p>Notifications In the case of a Personal Data breach, the controller must notify the supervisory authority of the breach. This must be done without due delay and, where feasible, not later than 72 hours after having become aware of it. (Article 33)</p> <p>Record keeping Each controller must maintain a record of its Processing activities. (Article 30)</p> <p>Appoint a representative The controller must appoint an EU representative in certain situations. (Article 27)</p> <p>Appoint a DPO The controller must appoint a Data Protection Officer (DPO) in certain situations. (Article 37(1))</p>	<p>Sensitive Personal Data may be processed if the data controller applies adequate safeguards with respect to the Processing of the sensitive data. (Article 10(2)(b))</p> <p>The controller must comply with the requirements in Articles 11 and/or 12 when transferring Personal Data out of the DIFC. (See below in 'Cross-border data transfers' section).</p> <p>Technical & organisational measures The controller is responsible for implementing appropriate technical and organisational measures to protect Personal Data. (Article 16(1))</p> <p>Data subject rights The controller must provide Data Subjects with at least the following information when collecting Personal Data:</p> <ul style="list-style-type: none"> • The identity of the controller • The purposes for Processing the Personal Data • Any further information which is necessary having regard to the specific circumstances (Article 13(1)) <p>Where Personal Data are not obtained from the Data Subject, a data controller or their representative must, at the time of undertaking the Processing, or if a disclosure to a third party is envisaged, no later than the time when the Personal Data are first processed or disclosed, provide the Data Subject with:</p> <ul style="list-style-type: none"> • the identity of the controller; 	<p>Technical & organisational measures The controller is responsible for implementing appropriate technical and organisational measures to protect Personal Data. (Article 9(1))</p> <p>Data subject rights The controller must provide Data Subjects with at least the following information when collecting Personal Data:</p> <ul style="list-style-type: none"> • The identity of the controller • The purposes of the Processing • Any further information that is necessary having regard to the specific circumstances in which the data are collected. (Article 6) <p>Where Personal Data are not obtained from the Data Subject, a data controller or their representative must, at the time of undertaking the Processing, or if a disclosure to a third party is envisaged, no later than the time when the Personal Data are first processed or disclosed, provide the Data Subject with:</p> <ul style="list-style-type: none"> • the identity of the controller; • the purposes of Processing; and • Any further information as necessary. (Article 7) <p>The controller must ensure that they can comply with the Data Subject rights as set out in Articles 10 and 11. (See below Data Subject Rights section)</p> <p>Choosing a data processor The controller is responsible for choosing a data processor that provides sufficient</p>	

GDPR	DIFC Laws	ADGM Laws	General Observations
	<ul style="list-style-type: none"> the purposes of Processing; and Any further information as necessary. (Article 14(1)) <p>The controller must ensure that they can comply with the Data Subject rights as set out in Articles 17 and 18. (See below in 'Data Subject Rights' section).</p> <p>Choosing a data processor The controller is responsible for choosing a data processor that provides sufficient technical and organisational guarantees and ensures compliance with these. (Article 16(3))</p> <p>Notifications The controller must inform the Commissioner of Data Protection (CDP) in the event of an unauthorised intrusion to any Personal Data database, as soon as reasonably practicable. (Article 16(4))</p> <p>The controller must file a notification with the CDP in accordance with the Data Protection Regulations (DPR). (Regulation 6.3.1)</p> <p>Record keeping The controller must keep records of any Personal Data Processing operations and must notify the CDP of any changes to these particulars. (Article 19 and Article 21, Regulation 6.3.2 and 6.3.3)</p> <p>Act only on instructions The processor must not process the Personal Data except on instructions from the controller, unless required to do so by law. (Article 15)</p>	<p>technical and organisational guarantees and ensures compliance with these. (Article 9(3))</p> <p>Registration A controller must notify the Registrar of its intention to become a Data Controller so that the Registrar can register them as such. This notification must be submitted to the Registrar on an annual basis where the Personal Data Processing is to continue in the subsequent year. (Article 12)</p> <p>Notifications A controller must notify the Registrar of:</p> <ul style="list-style-type: none"> The appointment of a data processor, within one month of the appointment; The cessation of a data processor, within one month of the cessation; Any change in the particulars of any data processor, within one month of the change; and Any change in its business contact details, within one month of the change. (Article 12(3)) <p>These notifications must be submitted to the registrar on an annual basis. (Article 12(4))</p> <p>The controller must inform the Registrar in the event of an unauthorised intrusion (including any loss of devices containing Personal Data or unauthorised disclosures), whether physical, electronic or otherwise, to any Personal Data, including by any of its data processors, of the incident without undue delay, and</p>	

GDPR		DIFC Laws	ADGM Laws	General Observations
		Notification The processor must inform the CDP of any unauthorised intrusion, either physical, electronic or otherwise to any Personal Data database. (Article 16(4))	where feasible, not later than 72 hours after becoming aware of it. (Article 9(5)) Record keeping The controller must keep records of any Personal Data Processing operations or set of operations intended to secure a single purpose or several related purposes. (Article 12(1))	
Data Subject Rights	Transparent communication In order to ensure that Personal Data are processed fairly and lawfully, controllers must provide certain minimum information to Data Subjects, regarding the collection and further Processing of their Personal Data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. (Articles 5(1)(a), 12-14) Data subject rights Data controllers have a legal obligation to give effect to the rights of Data Subjects. (Article 12(2)) Identifying data subjects Data controllers must not refuse to give effect to the rights of a Data Subject unless the controller cannot identify the Data Subject. The controller must use all reasonable efforts to verify the identity of Data Subjects. Where the controller has reasonable doubts as to the identity of the Data Subject, the controller may request the provision of additional information necessary to confirm the identity of the Data Subject, but is not required to do so. (Article 12(2), (6))	Right to access to and rectification, erasure or blocking of personal data Data Subjects have the right to obtain from the data controller, upon request, at reasonable intervals and without excessive delay or expense: <ul style="list-style-type: none"> Confirmation as to whether his Personal Data is being processed and information about the purpose of such Processing, the categories of Personal Data concerned, and the recipients to whom the Personal Data are disclosed; A copy of the Personal Data being processed and any available information as to its source; and As appropriate, the rectification, erasure or blocking of Personal Data when the Processing of such does not comply with the law. (Article 17) Right to object to processing Data Subjects have the right to: <ul style="list-style-type: none"> object at any time on reasonable grounds to the Processing of his Personal Data; and to be informed before Personal Data is disclosed for the first time to third 	Right of access, rectification, erasure, blocking Data Subjects have the right to obtain from the data controller, upon request, at reasonable intervals and without excessive delay or expense: <ul style="list-style-type: none"> Confirmation as to whether his Personal Data is being processed and information about the purpose of such Processing, the categories of Personal Data concerned, and the recipients to whom the Personal Data are disclosed; A copy of the Personal Data being processed and any available information as to its source; and As appropriate, the rectification, erasure or blocking of Personal Data when the Processing of such does not comply with these regulations. (Article 10) Right to object to processing Data Subjects have the right to: <ul style="list-style-type: none"> object at any time on reasonable grounds to the Processing of his Personal Data; and 	Both the DIFC and ADGM, being based on the 1995 Directive, largely mirror the GDPR in terms of Data Subject rights. However, the GDPR expands on the rights contained in the 1995 Directive and creates several entirely new rights.

GDPR	DIFC Laws	ADGM Laws	General Observations
<p>Time limits A controller must, within one month of receiving a request made under those rights, provide any requested information in relation to any of the rights of Data Subjects. If the controller fails to meet this deadline, the Data Subject may complain to the relevant DPSA and may seek a judicial remedy. Where a controller receives large numbers of requests, or especially complex requests, the time limit may be extended by a maximum of two further months. (Article 12(3) - (4))</p> <p>Basic Information Data Subjects have the right to be provided with information on the identity of the controller, the reasons for Processing their Personal Data and other relevant information necessary to ensure the fair and transparent Processing of Personal Data. (Articles 13 and 14)</p> <p>Right of access Data Subjects have the right to obtain the following:</p> <ul style="list-style-type: none"> • confirmation of whether, and where, the controller is Processing their Personal Data; • information about the purposes of the Processing; • information about the categories of data being processed; • information about the categories of recipients with whom the data may be shared; • information about the period for which the data will be stored (or the criteria used to determine that period); 	<p>parties or for the purposes of direct marketing, and to be expressly given the right to object to such uses. (Article 18)</p>	<ul style="list-style-type: none"> • to be informed before Personal Data is disclosed for the first time to third parties or for the purposes of direct marketing, and to be expressly given the right to object to such uses. (Article 11) 	

GDPR	DIFC Laws	ADGM Laws	General Observations
	<ul style="list-style-type: none"> • information about the existence of the rights to erasure, to rectification, to restriction of Processing and to object to Processing; • information about the existence of the right to complain to the DPSA; • where the data were not collected from the Data Subject, information as to the source of the data; and • information about the existence of, and an explanation of the logic involved in any automated Processing that has a significant effect on Data Subjects; and • Data Subjects may request a copy of the Personal Data being processed. (Article 15) <p>Access fees Data controllers must give effect to the rights of access, rectification, erasure and the right to object, free of charge. The controller may charge a reasonable fee for "repetitive requests", "manifestly unfounded or excessive requests" or "further copies". (Articles 12(5), 15(3), (4))</p> <p>Rectification Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data Subjects have the right to rectification of inaccurate Personal Data. (Articles 5(1)(d), 16)</p> <p>Erasure Data Subjects have the right to erasure of Personal Data if:</p> <ul style="list-style-type: none"> • the data are no longer needed for their original purpose (and no new lawful purpose exists); 		

GDPR	DIFC Laws	ADGM Laws	General Observations
	<ul style="list-style-type: none"> the lawful basis for the Processing is the Data Subject's consent, the Data Subject withdraws that consent, and no other lawful ground exists; the Data Subject exercises the right to object, and the controller has no overriding grounds for continuing the Processing; the data have been processed unlawfully; or erasure is necessary for compliance with EU law or the national law of the relevant Member State. (Article 17) <p>Restrict processing Data Subjects have the right to restrict the Processing of Personal Data (meaning that the data may only be held by the controller, and may only be used for limited purposes) if:</p> <ul style="list-style-type: none"> the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); the Processing is unlawful and the Data Subject requests restriction (as opposed to exercising the right to erasure); the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or if verification of overriding grounds is pending, in the context of an erasure request. (Article 18) <p>Portability Data Subjects have a right to:</p>		

GDPR	DIFC Laws	ADGM Laws	General Observations
<ul style="list-style-type: none"> • receive a copy of their Personal Data in a structured, commonly used, machine-readable format that supports re-use; • transfer their Personal Data from one controller to another; • store their Personal Data for further personal use on a private device; and • have their Personal Data transmitted directly between controllers without hindrance. (Article 20) <p>Object to processing Data Subjects have the right to object, on grounds relating to their particular situation, to the Processing of Personal Data, where the basis for that Processing is either:</p> <ul style="list-style-type: none"> • public interest; or • legitimate interests of the controller. <p>The controller must cease such Processing unless the controller:</p> <ul style="list-style-type: none"> • demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject; or • requires the data in order to establish, exercise or defend legal rights. (Article 21) <p>Where Personal Data are processed for scientific and historical research purposes or statistical purposes, the Data Subject has the right to object, unless the Processing is necessary for the performance of a task carried out for reasons of public interest. (Articles 21(6), 83(1))</p>			

GDPR		DIFC Laws	ADGM Laws	General Observations
	<p>Object to direct marketing Data Subjects have the right to object to the Processing of Personal Data for the purpose of direct marketing, including profiling. (Article 21(2) – (3))</p> <p>Duty to inform of right to object The right to object to Processing of Personal Data noted above must be communicated to the Data Subject no later than the time of the first communication with the Data Subject.</p> <p>This information should be provided clearly and separately from any other information provided to the Data Subject. (Articles 3(2)(b), 14(2)(c), 15(1)(e), 21(4))</p> <p>Automated processing Data Subjects have the right not to be subject to a decision based solely on automated Processing which significantly affect them (including profiling). Such Processing is permitted where:</p> <ul style="list-style-type: none"> • it is necessary for entering into or performing a contract with the Data Subject provided that appropriate safeguards are in place; • it is authorised by law; or • the Data Subject has explicitly consented and appropriate safeguards are in place. (Article 22) 			
Cross-Border Transfer Rules	<p>General prohibition Cross-Border Personal Data Transfers may only take place if the transfer is made to an Adequate Jurisdiction or the data exporter has implemented a lawful data transfer mechanism (or an exemption or derogation applies). (Articles 44, 45)</p>	<p>General prohibition Data controllers may transfer Personal Data out of the DIFC if the Personal Data is being transferred to a recipient in a jurisdiction that has laws that ensure an adequate level of protection for that Personal Data (pursuant to the Data</p>	<p>General prohibition Transfers of Personal Data to recipients located in a jurisdiction outside the ADGM may only take place if either:</p>	<p>The rules surrounding Cross-border data transfers in both the DIFC and ADGM, being based on the 1995 Directive, mirror to a significant extent those in the GDPR. The GDPR however, whilst maintaining the existing data transfer mechanisms created under the 1995 Directive (with</p>

GDPR	DIFC Laws	ADGM Laws	General Observations
<p>Adequacy decisions Cross-border data transfers may take place if the third country receives an Adequacy Decision from the EU Commission. (Articles 44, 45)</p> <p>The EU Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the USA (subject to compliance with the terms of the US-EU Privacy Shield).</p> <p>Public authorities Cross-border data transfers between public authorities may take place under agreements between public authorities, which do not require any specific authorisation from a DPSA. (Articles 46(2)(a), 46(3)(b))</p> <p>Binding Corporate Rules Cross-border data transfers within a corporate group may take place on the basis of Binding Corporate Rules ("BCRs"). BCRs require approval from DPSAs, but approved, individual transfers made under the BCRs do not require further approval. (Articles 4(20) 46(2)(b), 47)</p> <p>Model clauses Cross-border data transfers may take place on the basis of the Model Clauses entered into between the data exporter and data recipient. Existing Model Clauses implemented under the 1995 Directive remain valid until amended, replaced or repealed under the GDPR. (Articles 28(6)-(8), 46(2)(c), 57(1)(j), (r), 93(2))</p>	<p>Protection Regulations ("DPR")) or any other jurisdiction approved by the Commissioner of Data Protection ("CDP"). (Article 11, Appendix 3 DPR)</p> <p>In the absence of an adequate level of protection, data controllers may transfer Personal Data out of the DIFC if:</p> <ul style="list-style-type: none"> The CDP has granted a permit of written authorisation for the transfer and the controller applies adequate safeguards with respect to the protection of Personal Data. The DPR then sets out the requirements for applying for this permit. The Data Subject has given their written consent for the proposed transfer. The transfer is necessary for the conclusion or performance of a contract between the Data Subject and data controller or the implementation of pre-contractual measures taken in response to the Data Subject's request. 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. 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. Transfer is necessary in order to protect the vital interests of the Data Subject. Transfer is made from a register intended to provide information to the 	<ul style="list-style-type: none"> the transfer is made to a jurisdiction which has been deemed 'adequate' by the Registrar; or any of the conditions in article 5 apply. (Article 4) <p>Article 5 states that in the absence of an adequacy decision, data may be transferred out of the ADGM if:</p> <ul style="list-style-type: none"> The Registrar has granted a permit for the transfer or the set of transfers and the data controller applies adequate safeguards with respect to the protection of such Personal Data (Article 5(1)(a)) The Data Subject has given his written consent to the proposed transfer (Article 5(1)(b)) The transfer is necessary for the performance of a contract between the Data Subject and the data controller or the implementation of pre-contractual measures taken in response to the Data Subject's request (Article 5(1)(c)) 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 (Article 5(1)(d)) The transfer is necessary for the establishment, exercise or defence of legal claims (Article 5(1)(e)) The transfer is necessary in order to protect the vital interests of the Data Subject (Article 5(1)(f)) The transfer is necessary in the interests of the ADGM (Article 5(1)(g)) 	<p>some minor amendments), also creates a number of new transfer mechanisms.</p> <p>In both the DIFC and ADGM, determining whether a jurisdiction maintains adequate levels of data protection rests with the respective regulators, both of whom have published lists of adequate data protection regimes. These include most European jurisdictions and a handful of other countries, but not the wider UAE.</p> <p>The ADGM Regulations include at Schedules 1 and 2 a sets of model clauses for Cross-border data transfers between both controller to controller and controller to processor. Such clauses appear to mirror the EU Standard Contractual Clauses.</p> <p>NOTE: Under the GDPR, Cross-border data transfers may take place on the basis of standard data protection clauses approved by the EU Commission ("Model Clauses"). The current set of Model Clauses are currently being challenged as a form of appropriate data transfer mechanism; therefore their future is uncertain.</p> <p>In January 2019, the Irish Supreme Court (as part of the <i>Schrems v Facebook</i> litigation) heard an appeal by Facebook over a decision of the Irish High Court to refer a number of questions to the Court of Justice of the EU ("CJEU") regarding the validity of this data transfer mechanism. The Supreme Court will publish its decision in due course. If Facebook is unsuccessful in its appeal, the CJEU will rule on these questions,</p>

GDPR	DIFC Laws	ADGM Laws	General Observations
<p>Other mechanisms Cross-border data transfers may take place on the basis, <i>inter alia</i>, of:</p> <ul style="list-style-type: none"> • standard data protection clauses adopted by one or more DPSAs under the GDPR. (Articles 46(2)(d), 64(1)(d), 57(1)(j), (r), 93(2)) • an approved code of conduct, together with binding and enforceable commitments to provide appropriate safeguards. (Articles 40, 41, 46(2)(e)) • certifications together with binding and enforceable commitments of the data importer to apply the certification to the transferred data. (Articles 42, 43, 46(2)(f)) • ad hoc clauses conforming to the GDPR and approved by the relevant DPSA. (Articles 46(3)(a), (4), 63)) • administrative arrangements between public authorities (e.g., MOUs) subject to DPSA approval. (Articles 46(3)(b), (4), 63) <p>Derogations Cross-border data transfers may be made on the basis, <i>inter alia</i>, that:</p> <ul style="list-style-type: none"> • the Data Subject explicitly consents having been informed of the possible risks of such transfer. (Article 49(1)(a), (3)) • the performance of a contract between the Data Subject and the controller. (Article 49(1)(b), (3)) • it is necessary for the purposes of performing or concluding a contract in the interests of the Data Subject. (Article 49(1)(c), (3)) • the transfer is necessary for important reasons of public interest. (Article 49(1)(d), (4)) 	<p>public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.</p> <ul style="list-style-type: none"> • Transfer is necessary for compliance with a legal obligation. • Transfer is necessary to uphold the legitimate interests of the data controller recognised in the international financial markets. • 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. (Article 12(1), Article 5 DPR) 	<ul style="list-style-type: none"> • The transfer is made at the request of a regulator, the police or other government agency (Article 5(1)(h)) • The transfer is made from a register which according to law 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 (Article 5(1)(i)) • The transfer is necessary for compliance with any regulatory or legal obligation to which the data controller is subject (Article 5(1)(j)) • The transfer is necessary to uphold the legitimate interests of the data controller recognised in the international financial markets, provided that the transfer is carried out in accordance with applicable standards and except where such interests are overridden by legitimate interests of the Data Subject relating to the Data Subject's particular situation (Article 5(1)(k)) • The transfer is necessary to comply with any regulatory, auditing, accounting, anti-money laundering or counter-terrorist financing obligations that apply to a data controller which is established in the ADGM, or for the prevention or detection of any crime (Article 5(1)(l)) • To a person established outside the ADGM who would be a data controller (if established in the ADGM) or who is a data processor, 	<p>which may result in a declaration that the Model Clauses are no longer valid as a transfer mechanism.</p>

GDPR		DIFC Laws	ADGM Laws	General Observations
	<ul style="list-style-type: none"> it is necessary for the purposes of legal proceedings, or obtaining legal advice. (Article 49(1)(e)) the transfer is necessary in order to protect the vital interests of the Data Subject, where the Data Subject is incapable of giving consent. (Article 49(1)(f)) the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by those of the individual subject to informing the relevant DPSA and the Data Subjects. (Article 49(1), (3), (6)) 		<p>if, prior to the transfer, a legally binding agreement in the form set out in Schedule 1 or Schedule 2 respectively of the DPR 2015 has been entered into between the transferor and recipient (Article 5(1)(m))</p> <ul style="list-style-type: none"> The transfer is made between members of a company group in accordance with a global data protection compliance policy of that group, under which all the members of such group that are or will be transferring or receiving the Personal Data are bound to comply with all the provisions of the ADGM Data Protection Regulations as if such group members were established in the ADGM (i.e., effectively, Binding Corporate Rules) (Article 5(1)(n)) 	
Personal Data Security	<p>Security Data controllers must implement appropriate technical and organisational security measures to protect Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.</p> <p>Depending on the nature of the Processing, these measures may include:</p> <ul style="list-style-type: none"> encryption of the Personal Data; on-going reviews of security measures; redundancy and back-up facilities; and regular security testing. (Article 32) 	<p>Appropriate technical & organisational measures Data controllers must implement appropriate technical and organisational measures. These measures should 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. This should be of particular consideration where sensitive Personal Data are being processed or where the Personal Data is being transferred out of the DIFC (to a jurisdiction without an adequate level of protection). (Article 16(1))</p> <p>The level of security should be of an appropriate level to the risks represented by the Processing and the nature of the</p>	<p>Appropriate technical & organisational measures Data controllers must implement appropriate technical and organisational measures. These measures should protect the data against unauthorised or unlawful Processing, and against accidental loss or destruction of, or damage to, the Personal Data. (Article 9(1))</p> <p>The level of security should be of an appropriate level to the risks represented by the Processing and the nature of the Personal Data being processed. (Article 9(2))</p> <p>Sufficient guarantees Data controllers must choose data processors who can provide sufficient guarantees in respect of technical security measures and organisational</p>	Being based on the 1995 Directive, the DIFC and ADGM Laws leave a significant amount of discretion to the controller in terms of the technical and organisational measures to be implemented in the controller's particular context. The GDPR is more prescriptive but the net effect is very similar.

GDPR		DIFC Laws	ADGM Laws	General Observations
		Personal Data being processed. (Article 16(2))	measures and who ensure compliance with these measures. (Article 9(3)) Notifications In the event of an unauthorised intrusion or disclosure, the data controller must inform the Registrar without undue delay, and where feasible, not later than 72 hours after becoming aware of it. (Article 9(5))	
Administrative Fines and Regulatory Sanctions	Judicial remedies Data Subjects have the right to an effective judicial remedy against: <ul style="list-style-type: none"> • decisions of a DPSA concerning them; • any failure by a DPSA to deal with, or respond to, a complaint within three months; and • any unlawful Processing of their Personal Data by a controller or processor. (Article 78-79) 	Commissioner of Data Protection If after investigation, the CDP is satisfied that there is evidence of a breach by the data controller, the CDP may issue a direction to the data controller requiring it to do either or both of the following: <ul style="list-style-type: none"> • Do or refrain from doing any act or thing within such time as may be specified in the direction. • Refrain from Processing any Personal Data specified in the direction or to refrain from Processing Personal Data for a purpose or in a manner specified in the direction. (Article 33(1)) 	Office of Data Protection: The Office of Data Protection has the power to: <ul style="list-style-type: none"> • Issue directions or warnings and make recommendations to controllers. (Article 14(3)(d)) • Impose fines in the event of non-compliance with these directions of up to \$25,000. (Article 14(3)(e) and 17(3)) <p>If the Office of Data Protection is satisfied that a controller has contravened or is contravening the Regulations, it may issue a direction to the controller. The direction will require it do either or both of the following:</p> <ul style="list-style-type: none"> • To do or refrain from doing any act or thing within a specified time. • To refrain from Processing any Personal Data specified in the direction or to refrain from Processing Personal Data for a purpose or in a manner specified in the direction. (Article 17(1)) 	Whereas the remedies and sanctions available under the DFIC and ADGM Laws are comparatively low, the remedies and sanctions available to DPSAs under the GDPR are significantly greater. Under the GDPR, DPSAs are considered to have more significant enforcement powers.
	Compensation & liability A Data Subject who has suffered harm as a result of the unlawful Processing of his or her Personal Data has the right to receive compensation from the controller or processor for the harm suffered: <ul style="list-style-type: none"> • Any controller involved in the Processing is liable for the harm caused. • A processor is liable for the harm caused by any of its (or its sub-processor's) Processing activities that are not in compliance with its obligations under the GDPR, or are in breach of the controller's instructions. • To ensure effective compensation, each controller or processor will be 	Fines A data controller that fails to comply with a direction of the CDP may be subject to fines and liable for payment of compensation. (Article 36, Regulation 7) Orders Additionally, if the CDP considers that a data controller or any officer of it has failed to comply with a direction, he may apply to the Court for one or more of the following orders:		

GDPR	DIFC Laws	ADGM Laws	General Observations
	<p>held liable for the entirety of the harm caused, if they are involved in the same Processing and responsible for that harm. (Article 82(1)-(2), (4))</p> <p>Joint-controller liability Data Subjects are entitled to enforce their rights against any of the joint controllers. Each joint controller is liable for the entirety of the damage, although national law may apportion liability between them. If one joint controller has paid full compensation, it may then bring proceedings against the other joint controllers to recover their portions of the damages. (Article 26(3), 82(3)-(5))</p> <p>Exemptions from liability A controller or processor is exempt from liability if it proves that it is not responsible for the event giving rise to the harm. There is no mention of force majeure events. (Article 82(3))</p> <p>Administrative fines The maximum fine that can be imposed for serious infringements of the GDPR is the greater of €20 million or 4% of an undertaking's worldwide turnover for the preceding financial year. (Article 83(5) – (6))</p> <p>Fine criteria When deciding whether to impose a fine and deciding on the amount, DPSAs are required to give due regard to a range of issues, including:</p> <ul style="list-style-type: none"> the nature, gravity and duration of the infringement; 	<ul style="list-style-type: none"> An order directing the data controller or officer to comply with the direction or any provision of the Law or the Regulations or of any legislation administered by the CDP relevant to the issue of the direction. An order directing the data controller or officer to pay any costs incurred by the CDP or other person relating to the issue of the direction by the CDP or the contravention of such law, Regulations or legislation relevant to the issue of the direction. Any other order that the Court considers appropriate. (Article 33) <p>Any data controller who is found to contravene the DIFC Laws or a direction of the CDP may appeal to the DIFC Court within 30 days. The DIFC Court may make any orders that it thinks just and appropriate in the circumstances, including remedies for damages, penalties or compensation. (Article 37)</p>	<p>Right to appeal A controller who receives a fine for its contravention of the ADGM Laws may refer such matter to the ADGM courts for review to contest either the issue of the fine or the amount. (Article 17(C))</p>

GDPR		DIFC Laws	ADGM Laws	General Observations
	<ul style="list-style-type: none"> the number of Data Subjects affected and the level of harm suffered by them; the intentional or negligent character of the infringement; any action taken by the controller or processor to mitigate the harm; any relevant previous infringements by the controller or processor; the degree of co-operation with the relevant DPSA; whether the infringement was self-reported by the controller or processor; and any other aggravating or mitigating factors. (Article 82(3)) 			
Role and Powers of any relevant Data Protection Supervisory Authority	<p>Independence DPSAs must act independently and operate free from all outside influences, including government control. (Article 52)</p> <p>Tasks The tasks of DPSAs include obligations to:</p> <ul style="list-style-type: none"> monitor and enforce the application of the GDPR; promote awareness of the risks, rules, safeguards and rights pertaining to Personal Data (especially in relation to children); advise national and governmental institutions on the application of the GDPR; hear claims brought by Data Subjects or their representatives, and inform Data Subjects of the outcome of such claims; 	<p>Role The CDP is essentially the regulating body in the DIFC and oversees the enforcement of the DIFC Laws. (Article 26)</p> <p>Powers The CDP needs to conduct all reasonable and necessary inspections and investigations before notifying a data controller that it has breached or is breaching the DIFC Laws or any regulations. (Article 33)</p>	<p>Role The Office of Data Protection, which forms a part of the Registrar, is the official body with day-to-day responsibility for enforcement and administration of the ADGM Laws. (Article 14)</p> <p>Powers The Office of Data Protection has the power to enforce regulatory sanctions and fines (as set out above). (Article 17 and 17A)</p>	Under the GDPR, DPSAs are considered to have more significant supervisory and enforcement powers than set out in the DIFC or ADGM Laws.

GDPR		DIFC Laws	ADGM Laws	General Observations
	<ul style="list-style-type: none"> • establish requirements for Impact Assessments; • encourage the creation of Codes of Conduct and review certifications; • authorise Model Clauses and BCRs; • keep records of sanctions and enforcement actions; and • fulfil "any other tasks related to protection of Personal Data". (Article 55, 57) <p>Powers DPSAs are empowered to oversee enforcement of the GDPR, investigate breaches of the GDPR and bring legal proceedings where necessary. (Article 58)</p>			

SAUDI ARABIA





Saudi Arabia – Executive summary

There is currently no specific data protection legislation in place in Saudi Arabia (**KSA**). However, media reports suggest that a new freedom of information and protection of private data law is under review by the formal advisory body of the KSA, the Shura Council.

Personal Data and privacy are protected in part by general Shari'a principles which prohibit the divulging of another's individual information to a third party without consent. Neither the Holy Qur'an nor the Sunna (the traditional portion of Muslim law based on Prophet Muhammad's (PBUH)) words or acts specify any penalties to be imposed for a violation of privacy or Personal Data. Rather, penalties are determined by a judge according to his own fair and just personal assessment of the case and may range from a fine to suspension from professional practice.

The Basic Law of Governance of the KSA broadly protects the privacy of individuals by stating that property, capital, and labour are basic constituents of the economic and social structure of the Kingdom and are protected by personal rights that perform a social function in accordance with Islamic sharia law. Telegraphic, postal, telephone and other means of communications are safeguarded and cannot be confiscated, delayed, read or breached.

The recently published KSA Ministry of Commerce and Industry Draft Regulations on Electronic Commerce also require a vendor to keep the personal information of the buyer, and any records of electronic

communications with the client, safe whether the same are under its own custody or control, or transferred to the vendors' agents or employees. The draft law also makes the vendor responsible for recordkeeping and requires it to take reasonable steps to ensure that such data is protected in an appropriate manner. The draft regulations are pending, and have not yet come into effect.

The *Electronic Transactions Law* (Royal Decree No M/18 of 8/3/1428H) imposes certain obligations on an internet service provider ("**ISP**") stating that the ISP and its staff must maintain confidentiality of information obtained in the course of business. The *Anti-Cyber Crime Law* (Royal Decree No M/17 of 8/3/1428H) aims to ensure information security, protection of rights pertaining to the legitimate use of computers and information networks, protection of public interest, morals and protection of the national economy. Similarly, the *Telcom Act* (Royal Decree No M/12 of 12/03/1422H) states that the privacy and confidentiality of telephone calls and information transmitted or received through public telecommunications networks shall be maintained and not disclosed save as permitted by law.

In 2018, the Saudi Communications and Information Technology Commission issued a novel and innovative regulatory framework for cloud computing (**Cloud Framework**). The Cloud Framework is based on the best international practice and public consultation analysis and governs the rights and obligations of cloud service providers, individual customers, government entities and businesses. The Cloud Framework represents one of only a few examples of cloud-specific regulatory frameworks around the world.

	GDPR	Electronic Transactions Law	Anti-Cyber Crime Law	General Observations
Principles of Data Processing	<p>Lawfulness, fairness, transparency Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. (Article 5(1)(a))</p> <p>Specified purposes Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. (Article 5(1)(b))</p> <p>Data minimisation Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. (Article 5(1)(c))</p> <p>Accuracy Personal Data must be accurate and, where necessary, kept up to date. (Article 5(1)(d))</p> <p>Storage limitation Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. (Article 5(1)(e))</p> <p>Integrity and confidentiality Personal Data must be processed in a way 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. (Article 5(1)(f))</p>	<p>Lawful basis A certification service provider shall observe the following:</p> <ul style="list-style-type: none"> maintain the confidentiality of information obtained in the course of business, excluding information that certificate holders permit – in written or electronic form - to be published or disclosed, or as provided for by law; and obtain applicant's personal information, directly or indirectly, with the applicant's written consent. (Article 18) 	<p>Lawful basis An individual's consent must be obtained in order to process their Personal Data including disclosing any documents obtained by such Processing.</p>	<p>The term 'Personal Data' is not defined in any law or regulation. Similarly, there are no formal notification or registration requirements before the Processing of data. A 'data controller' is not defined in any law or regulation in the KSA.</p> <p>Status There is currently no specific data protection legislation in place in the KSA. The Electronic Transactions Law imposes certain obligations in respect of obtaining Personal Data and maintaining the confidentiality thereof but only applies to electronic transactions.</p> <p>Looking forward Media reports suggest that a new freedom of information and protection of private data law is under review by the formal advisory body of the KSA, the Shura Council. Very limited information is available about this law.</p>

	GDPR	Electronic Transactions Law	Anti-Cyber Crime Law	General Observations
	<p>Accountability The controller shall be responsible for and be able to demonstrate compliance with all the above principles. (Article 5(2))</p> <p>Lawful bases The legal bases under which Personal Data may be processed are:</p> <ul style="list-style-type: none"> • with the freely given, specific, informed and unambiguous consent of the Data Subject; • where necessary for the performance of a contract to which the Data Subject is party; • where necessary to comply with a legal obligation to which the controller is subject; • where necessary to protect the vital interests of the Data Subject or another person; • where 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 • where necessary for the purposes of the legitimate interests of the controller or a third party. (Article 6(1)) 			
Data Controller and Data Processor Obligations	<p>General principles The controller is responsible for compliance with the principles listed in Article 5 (as set out above).</p> <p>The controller must have regard to 'data protection by design and by default' throughout their Processing activities.</p> <p>Lawful processing The controller must carry only process Personal Data under one of the conditions</p>	<p>Confidentiality A certification service provider shall maintain the confidentiality of information obtained in the course of business, excluding information that certificate holders permit – in written or electronic form - to be published or disclosed, or as provided for by law. (Article 18)</p> <p>Consent A certification service provider shall obtain applicant's personal information, directly or</p>	<p>Lawful basis An individual's consent must be obtained in order to process their Personal Data including disclosing any documents obtained by such Processing.</p>	<p>The GDPR places significantly more onerous burdens on Data Controllers and Data Processors than any law in the KSA.</p> <p>Data Processing agreements are not governed by any laws or regulations in the KSA. No standard form or precedent data Processing agreements have been approved by the national authorities or KSA courts.</p>

GDPR	Electronic Transactions Law	Anti-Cyber Crime Law	General Observations
<p>laid out in Article 6 and for special categories of Personal Data those laid out in Article 9.</p> <p>Sensitive personal data The Processing of sensitive Personal Data is prohibited, unless the:</p> <ul style="list-style-type: none"> • Data Subject has given explicit consent. (Article 9(2)(a)) • Processing is necessary in the context of employment law, or laws relating to social security and social protection. (Article 9(2)(b)) • Processing is necessary to protect vital interests of the Data Subject (or another person). (Article 9(2)(c)) • Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim. (Article 9(2)(d)) • Processing relates to Personal Data which are manifestly made public by the Data Subject. (Article 9(2)(e)) • Processing is necessary for the establishment, exercise or defence of legal claims. (Article 9(2)(f)) • Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law. (Article 9(2)(g)) • Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or 	<p>indirectly, with the applicant's written consent. (Article 18)</p>		

GDPR	Electronic Transactions Law	Anti-Cyber Crime Law		General Observations
	<p>treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional. (Article 9(2)(h))</p> <ul style="list-style-type: none"> Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law. (Article 9(2)(i)) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. (Article 9(2)(j)) <p>Technical & organisational measures The controller is responsible for implementing appropriate technical and organisational measures to ensure and demonstrate that its Processing activities are compliant with the requirements of the GDPR. (Article 32)</p> <p>Data subject rights The controller must demonstrate the Data Subject's consent to Processing their Personal Data. The consent must be clearly presented and easily distinguished from other matters, in an intelligible and easily accessible form. The consent must be able to be withdrawn at any time. (Article 24)</p> <p>The controller must make reasonable efforts to verify parental consent (when the</p>			

GDPR	Electronic Transactions Law	Anti-Cyber Crime Law	General Observations
<p>child is under 16, although in some members states may be as young as 13).</p> <p>Choosing a data processor The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of this Regulation and ensure the protection of the rights of the Data Subject.</p> <p>Processing by a processor shall be governed by a contract or other legal act. (Article 28)</p> <p>Notifications In the case of a Personal Data breach, the controller must notify the supervisory authority of the breach. This must be done without due delay and, where feasible, not later than 72 hours after having become aware of it. (Article 33)</p> <p>Record keeping Each controller must maintain a record of its Processing activities. (Article 30)</p> <p>Appoint a representative The controller must appoint an EU representative in certain situations. (Article 27)</p> <p>Appoint a DPO The controller must appoint a Data Protection Officer (DPO) in certain situations. (Article 37(1))</p>			
<p>Data Subject Rights</p>	<p>Transparent communication In order to ensure that Personal Data are processed fairly and lawfully, controllers must provide certain minimum information</p>	<p>Lawful basis A certification service provider shall observe the following:</p>	<p>No specific relevant provisions exist.</p> <p>There is no general protection of Data Subject rights in line with the GDPR. Shari'a principles, the Constitution and the Electronic Transactions Law provide</p>

GDPR	Electronic Transactions Law	Anti-Cyber Crime Law	General Observations
<p>to Data Subjects, regarding the collection and further Processing of their Personal Data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. (Articles 5(1)(a), 12-14)</p> <p>Data subject rights Data controllers have a legal obligation to give effect to the rights of Data Subjects. (Article 12(2))</p> <p>Identifying data subjects Data controllers must not refuse to give effect to the rights of a Data Subject unless the controller cannot identify the Data Subject. The controller must use all reasonable efforts to verify the identity of Data Subjects. Where the controller has reasonable doubts as to the identity of the Data Subject, the controller may request the provision of additional information necessary to confirm the identity of the Data Subject, but is not required to do so. (Article 12(2), (6))</p> <p>Time limits A controller must, within one month of receiving a request made under those rights, provide any requested information in relation to any of the rights of Data Subjects. If the controller fails to meet this deadline, the Data Subject may complain to the relevant DPSA and may seek a judicial remedy. Where a controller receives large numbers of requests, or especially complex requests, the time limit may be extended by a maximum of two further months. (Article 12(3) - (4))</p>	<ul style="list-style-type: none"> maintain the confidentiality of information obtained in the course of business, excluding information that certificate holders permit – in written or electronic form - to be published or disclosed, or as provided for by law; and obtain applicant's personal information, directly or indirectly, with the applicant's written consent. (Article 18) 		<p>merely the right not to have their personal information captured without their consent and to have the confidentiality of such information maintained.</p>

GDPR	Electronic Transactions Law	Anti-Cyber Crime Law	General Observations
	<p>Basic information Data Subjects have the right to be provided with information on the identity of the controller, the reasons for Processing their Personal Data and other relevant information necessary to ensure the fair and transparent Processing of Personal Data. (Articles 13 and 14)</p> <p>Right of access Data Subjects have the right to obtain the following:</p> <ul style="list-style-type: none"> • confirmation of whether, and where, the controller is Processing their Personal Data; • information about the purposes of the Processing; • information about the categories of data being processed; • information about the categories of recipients with whom the data may be shared; • information about the period for which the data will be stored (or the criteria used to determine that period); • information about the existence of the rights to erasure, to rectification, to restriction of Processing and to object to Processing; • information about the existence of the right to complain to the DPSA; • where the data were not collected from the Data Subject, information as to the source of the data; and • information about the existence of, and an explanation of the logic involved in any automated Processing that has a significant effect on Data Subjects; and 		

GDPR	Electronic Transactions Law	Anti-Cyber Crime Law	General Observations
<ul style="list-style-type: none"> Data Subjects may request a copy of the Personal Data being processed. (Article 15) <p>Access fees Data controllers must give effect to the rights of access, rectification, erasure and the right to object, free of charge. The controller may charge a reasonable fee for "repetitive requests", "manifestly unfounded or excessive requests" or "further copies". (Articles 12(5), 15(3), (4))</p> <p>Rectification Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data Subjects have the right to rectification of inaccurate Personal Data. (Articles 5(1)(d), 16)</p> <p>Erasure Data Subjects have the right to erasure of Personal Data if:</p> <ul style="list-style-type: none"> the data are no longer needed for their original purpose (and no new lawful purpose exists); the lawful basis for the Processing is the Data Subject's consent, the Data Subject withdraws that consent, and no other lawful ground exists; the Data Subject exercises the right to object, and the controller has no overriding grounds for continuing the Processing; the data have been processed unlawfully; or erasure is necessary for compliance with EU law or the national law of the relevant Member State. (Article 17) 			

GDPR	Electronic Transactions Law	Anti-Cyber Crime Law	General Observations
	<p>Restrict processing Data Subjects have the right to restrict the Processing of Personal Data (meaning that the data may only be held by the controller, and may only be used for limited purposes) if:</p> <ul style="list-style-type: none"> • the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); • the Processing is unlawful and the Data Subject requests restriction (as opposed to exercising the right to erasure); • the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or • if verification of overriding grounds is pending, in the context of an erasure request. (Article 18) <p>Portability Data Subjects have a right to:</p> <ul style="list-style-type: none"> • receive a copy of their Personal Data in a structured, commonly used, machine-readable format that supports re-use; • transfer their Personal Data from one controller to another; • store their Personal Data for further personal use on a private device; and • have their Personal Data transmitted directly between controllers without hindrance. (Article 20) 		

GDPR	Electronic Transactions Law	Anti-Cyber Crime Law	General Observations
<p>Object to processing Data Subjects have the right to object, on grounds relating to their particular situation, to the Processing of Personal Data, where the basis for that Processing is either:</p> <ul style="list-style-type: none"> • public interest; or • legitimate interests of the controller. <p>The controller must cease such Processing unless the controller:</p> <ul style="list-style-type: none"> • demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject; or • requires the data in order to establish, exercise or defend legal rights. (Article 21) <p>Where Personal Data are processed for scientific and historical research purposes or statistical purposes, the Data Subject has the right to object, unless the Processing is necessary for the performance of a task carried out for reasons of public interest. (Articles 21(6), 83(1))</p> <p>Object to direct marketing Data Subjects have the right to object to the Processing of Personal Data for the purpose of direct marketing, including profiling. (Article 21(2) – (3))</p> <p>Duty to inform of right to object The right to object to Processing of Personal Data noted above must be communicated to the Data Subject no later than the time of the first communication with the Data Subject.</p>			

GDPR		Electronic Transactions Law	Anti-Cyber Crime Law	General Observations
	<p>This information should be provided clearly and separately from any other information provided to the Data Subject. (Articles 3(2)(b), 14(2)(c), 15(1)(e), 21(4))</p> <p>Automated processing Data Subjects have the right not to be subject to a decision based solely on automated Processing which significantly affect them (including profiling). Such Processing is permitted where:</p> <ul style="list-style-type: none"> • it is necessary for entering into or performing a contract with the Data Subject provided that appropriate safeguards are in place; • it is authorised by law; or • the Data Subject has explicitly consented and appropriate safeguards are in place. (Article 22) 			
Cross-Border Transfer Rules	<p>General prohibition Cross-Border Personal Data Transfers may only take place if the transfer is made to an Adequate Jurisdiction or the data exporter has implemented a lawful data transfer mechanism (or an exemption or derogation applies). (Articles 44, 45)</p> <p>Adequacy decisions Cross-border data transfers may take place if the third country receives an Adequacy Decision from the EU Commission. (Articles 44, 45)</p> <p>The EU Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the</p>	No specific relevant provisions exist.	No specific relevant provisions exist.	<p>There is no regulation currently dealing with the transfer of data outside the KSA. Data transfer agreements are not governed by any laws or regulations in the KSA. No standard form or precedent data transfer agreements have been approved by the national authorities or the KSA courts.</p> <p>NOTE: Under the GDPR, Cross-border data transfers may take place on the basis of standard data protection clauses approved by the EU Commission ("Model Clauses"). The current set of Model Clauses are currently being challenged as a form of appropriate data transfer mechanism; therefore their future is uncertain.</p>

GDPR	Electronic Transactions Law	Anti-Cyber Crime Law	General Observations
<p>USA (subject to compliance with the terms of the US-EU Privacy Shield).</p> <p>Public authorities Cross-border data transfers between public authorities may take place under agreements between public authorities, which do not require any specific authorisation from a DPSA. (Articles 46(2)(a), 46(3)(b))</p> <p>Binding Corporate Rules Cross-Border Data Transfer within a corporate group may take place on the basis of Binding Corporate Rules ("BCRs"). BCRs require approval from DPSAs, but approved, individual transfers made under the BCRs do not require further approval. (Articles 4(20) 46(2)(b), 47)</p> <p>Model clauses Cross-border data transfers may take place on the basis of the Model Clauses entered into between the data exporter and data recipient. Existing Model Clauses implemented under the 1995 Directive remain valid until amended, replaced or repealed under the GDPR. (Articles 28(6)-(8), 46(2)(c), 57(1)(j), (r), 93(2))</p> <p>Other mechanisms Cross-border data transfers may take place on the basis, <i>inter alia</i>, of:</p> <ul style="list-style-type: none"> • standard data protection clauses adopted by one or more DPSAs under the GDPR. (Articles 46(2)(d), 64(1)(d), 57(1)(j), (r), 93(2)) • an approved code of conduct, together with binding and enforceable commitments to provide appropriate safeguards. (Articles 40, 41, 46(2)(e)) 			<p>In January 2019, the Irish Supreme Court (as part of the <i>Schrems v Facebook</i> litigation) heard an appeal by Facebook over a decision of the Irish High Court to refer a number of questions to the Court of Justice of the EU ("CJEU") regarding the validity of this data transfer mechanism. The Supreme Court will publish its decision in due course. If Facebook is unsuccessful in its appeal, the CJEU will rule on these questions, which may result in a declaration that the Model Clauses are no longer valid as a transfer mechanism.</p>

GDPR	Electronic Transactions Law	Anti-Cyber Crime Law	General Observations
<ul style="list-style-type: none"> • certifications together with binding and enforceable commitments of the data importer to apply the certification to the transferred data. (Articles 42, 43, 46(2)(f)) • ad hoc clauses conforming to the GDPR and approved by the relevant DPSA. (Articles 46(3)(a), (4), 63)) • administrative arrangements between public authorities (e.g., MOUs) subject DPSA approval. (Articles 46(3)(b), (4), 63) <p>Derogations Cross-border data transfers may be made on the basis, <i>inter alia</i>, that:</p> <ul style="list-style-type: none"> • the Data Subject explicitly consents having been informed of the possible risks of such transfer. (Article 49(1)(a), (3)) • the performance of a contract between the Data Subject and the controller. (Article 49(1)(b), (3)) • it is necessary for the purposes of performing or concluding a contract in the interests of the Data Subject. (Article 49(1)(c), (3)) • the transfer is necessary for important reasons of public interest. (Article 49(1)(d), (4)) • it is necessary for the purposes of legal proceedings, or obtaining legal advice. (Article 49(1)(e)) • the transfer is necessary in order to protect the vital interests of the Data Subject, where the Data Subject is incapable of giving consent. (Article 49(1)(f)) • the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by those of the individual subject to informing the 			

GDPR		Electronic Transactions Law	Anti-Cyber Crime Law	General Observations
	relevant DPSA and the Data Subjects. (Article 49(1), (3), (6))			
Personal Data Security	<p>Security Data controllers must implement appropriate technical and organisational security measures to protect Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.</p> <p>Depending on the nature of the Processing, these measures may include:</p> <ul style="list-style-type: none"> • encryption of the Personal Data; • on-going reviews of security measures; • redundancy and back-up facilities; and • regular security testing. (Article 32) 	<p>Confidentiality A certification service provider shall maintain the confidentiality of information obtained in the course of business, excluding information that certificate holders permit – in written or electronic form - to be published or disclosed, or as provided for by law. (Article 18)</p>	No specific relevant provisions exist.	There are no specific provisions relating to Personal Data security outside the requirement to keep such data confidential under the Electronic Transactions Law.
Administrative Fines and Regulatory Sanctions	<p>Judicial remedies Data Subjects have the right to an effective judicial remedy against:</p> <ul style="list-style-type: none"> • decisions of a DPSA concerning them; • any failure by a DPSA to deal with, or respond to, a complaint within three months; and • any unlawful Processing of their Personal Data by a controller or processor. (Article 78-79) <p>Compensation & liability A Data Subject who has suffered harm as a result of the unlawful Processing of his or her Personal Data has the right to receive compensation from the controller or processor for the harm suffered:</p> <ul style="list-style-type: none"> • Any controller involved in the Processing is liable for the harm caused. 	<p>Offences It is an offence for a certification provider to:</p> <ul style="list-style-type: none"> • use information concerning the applicant, for purposes other than certification, without the applicant's consent in a written or electronic form; • disclosure information accessed by virtue of his work without the certificate holder's consent in a written or electronic form, or as provided for by law; • steal the identity of another person or falsely claim to represent him in applying for, accepting or requesting the suspension or revocation of a digital certificate. (Article 23) <p>Penalties Anyone found guilty of any offence under Article 23 of this Law shall be subject to:</p>	<p>Invasion of privacy Anyone who:</p> <ul style="list-style-type: none"> • spies on, interception or reception of data transmitted through an information network or a computer without legitimate authorisation; or • invades an individual's privacy through the misuse of camera-equipped mobile phones etc., <p>shall be subject to:</p> <ul style="list-style-type: none"> • imprisonment for a period not exceeding 1 year; and/or • a fine not exceeding 500,000 Riyals. (Article 3) 	<p>The absence of a national DPSA means that there is no effective supervision and/or enforcement of Data Subject rights or data protection principles in the KSA.</p> <p>Cybercrime is severely punishable by the KSA Ministry of Interior and the Communications and Information Technology Commission and penalties are imposed for identity theft, defamation, electronic piracy, email theft and other unlawful activities.</p>

GDPR	Electronic Transactions Law	Anti-Cyber Crime Law	General Observations
<ul style="list-style-type: none"> • A processor is liable for the harm caused by any of its (or its sub-processor's) Processing activities that are not in compliance with its obligations under the GDPR, or are in breach of the controller's instructions. • To ensure effective compensation, each controller or processor will be held liable for the entirety of the harm caused, if they are involved in the same Processing and responsible for that harm. (Article 82(1)-(2), (4)) <p>Joint-controller liability Data Subjects are entitled to enforce their rights against any of the joint controllers. Each joint controller is liable for the entirety of the damage, although national law may apportion liability between them. If one joint controller has paid full compensation, it may then bring proceedings against the other joint controllers to recover their portions of the damages. (Article 26(3), 82(3)-(5))</p> <p>Exemptions from liability A controller or processor is exempt from liability if it proves that it is not responsible for the event giving rise to the harm. There is no mention of force majeure events. (Article 82(3))</p> <p>Administrative fines The maximum fine that can be imposed for serious infringements of the GDPR is the greater of €20 million or 4% of an undertaking's worldwide turnover for the preceding financial year. (Article 83(5) – (6))</p> <p>Fine criteria When deciding whether to impose a fine and deciding on the amount, DPSAs are</p>	<ul style="list-style-type: none"> • imprisonment for a period not exceeding 5 years; and/or • a fine not exceeding 5million Riyals. (Article 24) <p>Confiscation Equipment, systems and programs used in committing the violation may be confiscated pursuant to a judgment. (Article 24)</p>	<p>Data destruction Any person who unlawfully accesses a computer with the intention to delete, erase, destroy, leak, damage, alter or redistribute private data shall be subject to:</p> <ul style="list-style-type: none"> • imprisonment for a period not exceeding 4 years; and/or • a fine not exceeding 3million Riyals. (Article 5) 	

GDPR		Electronic Transactions Law	Anti-Cyber Crime Law	General Observations
	<p>required to give due regard to a range of issues, including:</p> <ul style="list-style-type: none"> the nature, gravity and duration of the infringement; the number of Data Subjects affected and the level of harm suffered by them; the intentional or negligent character of the infringement; any action taken by the controller or processor to mitigate the harm; any relevant previous infringements by the controller or processor; the degree of co-operation with the relevant DPSA; whether the infringement was self-reported by the controller or processor; and any other aggravating or mitigating factors. (Article 82(3)) 			
Role and Powers of any relevant Data Protection Supervisory Authority	<p>Independence DPSAs must act independently and operate free from all outside influences, including government control. (Article 52)</p> <p>Tasks The tasks of DPSAs include obligations to:</p> <ul style="list-style-type: none"> monitor and enforce the application of the GDPR; promote awareness of the risks, rules, safeguards and rights pertaining to Personal Data (especially in relation to children); advise national and governmental institutions on the application of the GDPR; hear claims brought by Data Subjects or their representatives, and inform 	<p>Inspections The KSA Communications and Information Technology Commission is empowered to record and inspect violations. (Article 23)</p>	<p>The Communications and Information Technology Commission shall provide support and assistance to the specialised security authorities throughout the process of investigating crimes committed under this law. (Article 14)</p> <p>The KSA Bureau of Investigation and Public Prosecution is empowered to investigate and prosecute crimes under this law. (Article 15)</p>	<p>The absence of a national data protection supervisory authority means that there is no effective supervision and/or enforcement of Data Subject rights or data protection principles in the KSA.</p>

GDPR		Electronic Transactions Law	Anti-Cyber Crime Law	General Observations
	<p>Data Subjects of the outcome of such claims;</p> <ul style="list-style-type: none"> • establish requirements for Impact Assessments; • encourage the creation of Codes of Conduct and review certifications; • authorise Model Clauses and BCRs; • keep records of sanctions and enforcement actions; and • fulfil "any other tasks related to protection of Personal Data". (Article 55, 57) <p>Powers</p> <p>DPSAs are empowered to oversee enforcement of the GDPR, investigate breaches of the GDPR and bring legal proceedings where necessary. (Article 58)</p>			

Saudi Cloud Computing Regulatory Framework

In 2018, the Saudi Communications and Information Technology Commission (**CITC**) issued a very novel and innovative regulatory framework for cloud computing (**Cloud Framework**) in the KSA. The Cloud Framework is based on the best international practice and public consultation analysis and govern the rights and obligations of cloud service providers (**CSPs**), individual customers, government entities and businesses. A second version of the Cloud Framework was published in February 2019, replacing the 2018 version. The Cloud Framework represents one of only a few examples of cloud-specific regulatory frameworks around the world. Some of the provisions, such as security breach notification, are in line with the approach taken in the EU while others, such as the requirement to register with the CITC content classification are specific to the KSA.

The Cloud Framework binds CSPs who conclude agreements for cloud services with Cloud Customers resident or having an address in the KSA. The Cloud Framework also applies where a CSP is Processing or storing Cloud Customer information (which includes Personal Data) within the KSA and to the ownership, operation, or offering of access to datacentres or cloud systems in the KSA. Some of the most important features of the Cloud Framework from a data protection perspective are the cloud security requirements CSPs must adhere to - Cloud Customer information can be subject to different levels of information security, depending on the required level of preservation of the Cloud Customer information's confidentiality, integrity, and availability.

Security Level	Categories of Customer Content
Level 1	Non-sensitive customer content of individuals, or private sector companies, not subject to any sector-specific restrictions on the outsourcing of data.
Level 2	Sensitive customer content of individuals, private sector companies, not subject to any sector-specific restrictions on the outsourcing of data; and non-sensitive customer content from public authorities.
Level 3	Any customer content from private sector-regulated industries subject to a Level 3 categorisation by virtue of sector-specific rules or a decision by a regulatory authority; and sensitive customer content from public authorities.
Level 4	Highly sensitive or secret customer content belonging to relevant governmental agencies or institutions.

The Cloud Framework also sets out a number of statutory presumptions regarding how such customer information should be classified from an information security standpoint (unless the relevant customer has requested otherwise). These information security presumptions (by category of Cloud Customer) are:

- for natural persons with a residence in the KSA: Level 1 treatment of Customer Content;
- for private sector legal persons, such as companies, other corporate entities, associations or organisations incorporated or with a customer address in the KSA: Level 2 treatment of Customer Content;
- for any government or state services or agencies: Level 3 treatment of Customer Content; and
- for all other categories: Level 1 treatment of Customer Content.

Cloud Framework	General Observations
<p>Obligations on CSPs</p> <p>Security features CSPs must inform any Cloud Customer, upon his request, of the information security features offered by the CSP or applied to the Cloud Customer's Customer Content. CSPs may also satisfy this obligation by making such information available in online format for Cloud Customers. (Article 3.3.7)</p> <p>Disclosures to the CITC CSPs registered with the CITC must disclose to it:</p> <ul style="list-style-type: none"> the location and main features of any of its Datacenters that are located in the KSA; and the foreign country or countries of the location of any of its Datacenters used for the Processing, storage, transit or transfer of Personal Data of Cloud Customers that have a Residence or Customer Address in the KSA. (Article 3.3.10) <p>Disclosures to cloud customers CSPs must inform their Cloud Customers in advance whether, <i>inter alia</i>, their Personal Data will be transferred, stored or processed outside the KSA, permanently or temporarily. (Article 3.3.11)</p> <p>Breach notifications CSPs must inform Cloud Customers, without undue delay, of any security breach or information leakage that those CSPs become aware of, if such breach or leakage affects, or is likely to affect, <i>inter alia</i>, those Cloud Customers' Personal Data. (Article 3.3.12)</p> <p>CSPs must inform the CITC, without undue delay, of any security breach or information leakage that those CSPs become aware of, if such breaches or leakages affect, or are likely to affect:</p> <ul style="list-style-type: none"> any Level 3 Customer Content; the Customer Content (including Personal Data) of a significant number of Cloud Customers; or a significant number of persons in the KSA because of their reliance on one or more Cloud Customers' services that are affected by the security breach or information leakage. (Article 3.3.13) <p>CSPs must notify the CITC and/or any other authorised entity, without undue delay, if they become aware of the presence of any Cloud Customer Personal Data or other information on their Cloud System that may constitute a violation of the Anti-Cyber Crime Law. (Article 3.5.6)</p> <p>Third party data sharing Save as required to comply with the laws of a foreign jurisdiction in respect of a Cloud Customer subject to the laws of that jurisdiction, CSPs may not provide or authorise another party to provide to any third party (including, but not limited to, any individuals, legal entities, domestic or foreign government or public authorities) Cloud Customer Personal Data. (Article 3.4.2)</p>	<p>Interesting and novel aspects of the Cloud Framework include:</p> <ul style="list-style-type: none"> obligations to provide certain pre-contract information to Cloud Customers and to include certain minimum content in cloud service contracts; an express acknowledgement that CSPs will not be held liable for unlawful or infringing content stored on their systems, combined with a process enabling the CITC to require providers to take down such content; various restrictions on CSPs ability to limit contractual liability in relation to their customers, and a process whereby customer Personal Data stored in the cloud can be exempted from content filtering in the KSA, where the data are: <ul style="list-style-type: none"> not accessible by users in the KSA; or only available to users of a private cloud or users who are under the control of single organisation. <p>Penalties The scope and quantum of potential penalties for a violation of the Cloud Framework have not yet been specifically fleshed out by the CITC. Rather, the Cloud Framework provides that any violation of its provisions shall incur such penalties as the CITC may impose under CITC statutes, and may also incur penalties under other applicable laws in the KSA.</p> <p>Other applicable laws include, in particular, the Anti-Cyber Crime Law and the Electronic Transactions Law, and any laws or provisions that may amend or replace them in the future.</p> <p>CITC The CITC has numerous laws and regulations relating to a variety of technological fields in place so it is expected that further regulatory documents in the field of information communication technology (ICT) will be forthcoming.</p>

Cloud Framework		General Observations
	<p>Further processing Save as required to comply with the laws of a foreign jurisdiction in respect of a Cloud Customer subject to the laws of that jurisdiction, CSPs may not process or use such Personal Data for purposes other than those allowed under the Cloud Computing Agreement with the Cloud Customer concerned. (Article 3.4.2)</p> <p>A CSP's obligations under Article 3.4.2 shall not apply with regard to any Cloud Customer Personal Data that meets one of the following two conditions:</p> <ul style="list-style-type: none"> that CSP is required to disclose, transmit, process or use that Cloud Customer Personal Data under KSA law; or the Cloud Customer Personal Data are Level 1 or Level 2 Data, and the relevant Cloud Customer provides its express prior consent (whether in an 'opt-in' or an 'opt-out' form), which the Cloud Customer shall remain free to withdraw at any time in the future. (Article 3.4.3) <p>Information to be provided to cloud customers CSPs must ensure that certain information be included in their cloud contracts, including:</p> <ul style="list-style-type: none"> identification of the CSP, business address and full contact details; rules on handling of Cloud Customer Personal Data, including its Processing and processes to enable Personal Data to be retrieved by the Cloud Customer upon the Cloud Contract's termination; and a procedure for the resolution of Cloud Customer complaints. (Article 3.6.3) 	<p>Future The KSA has great ambition to become a more active competitor in the field of ICT. In the past, the numerous stakeholders involved could be seen to delay the drafting and enactment of legislation. However, recent revamps of various government departments indicate that significant reforms are soon to follow.</p> <p>It is reasonable to assume therefore that the Cloud Framework is just one of many first steps toward a clearer and more transparent regulatory approach in the ICT sector.</p>
Obligations on Cloud Customers	<p>Data sharing Cloud Customers are obliged to ensure that, if allowed, any outsourcing, transmission, Processing or storage should be subject to certain information security or data protection restrictions or safeguards, in addition to those specified to Cloud Framework. (Article 3.3.3.2)</p> <p>Information security Cloud Customers are responsible for:</p> <ul style="list-style-type: none"> selecting the appropriate information security level which best matches their specific needs, duties, obligations and security requirements. (Article 3.3.5) for implementing all information security features required for part or the whole of their Personal Data. (Article 3.3.6) <p>Cross-border data transfers Cloud Customers must ensure that no Level 3 Customer Content is transferred outside the KSA, for whatever purpose and in whatever format, whether permanently or temporarily (e.g. for caching,</p>	

Cloud Framework		General Observations
	<p>redundancy or similar purposes), unless this is expressly allowed under the laws or regulations of the KSA. (Article 3.3.8)</p> <p>Public clouds Cloud Customers may not transfer, store or process Level 3 Customer Content to or in any public, community or hybrid cloud unless and for as long as the CSP is validly registered with the CITC. (Article 3.3.9)</p> <p>Information to be provided CSPs must inform their Cloud Customers in advance whether their Customer Content will be transferred, stored or processed outside the KSA, permanently or temporarily. (Article 3.3.11)</p>	
Data Subject Rights	<p>Right of access CSPs shall grant Cloud Customers the right and the technical capability to access their Personal Data. (Article 3.4.4)</p> <p>Right of verification CSPs shall grant Cloud Customers the right and the technical capability to verify their Personal Data. (Article 3.4.4)</p> <p>Right of rectification CSPs shall grant Cloud Customers the right and the technical capability to correct their Personal Data. (Article 3.4.4)</p> <p>Right to erasure CSPs shall grant Cloud Customers the right and the technical capability to delete their Personal Data. (Article 3.4.4)</p> <p>Right to copies of personal data Upon termination of the Cloud Contract with a Cloud Customer, and if the Cloud Customer so requests, the CSP must:</p> <ul style="list-style-type: none"> provide to the Cloud Customer a copy of the Cloud Customer's Cloud Content stored on the CSP's Cloud System at the time of the Cloud Contract's termination, in a commonly used format, or allow and offer the Cloud Customer the means to download such Cloud Content, in a commonly used format. (Article 3.6.6) <p>The CSP may alternatively transfer the Cloud Customer's Personal Data, in a suitable format, directly to another CSP of the Cloud Customer's choice, where this is technically feasible. (Article 3.6.6)</p>	

Cloud Framework		General Observations
Cross-Border Transfer Rules	<p>Cross-border data transfers Cloud Customers must ensure that no Level 3 Customer Content is transferred outside the KSA, for whatever purpose and in whatever format, whether permanently or temporarily (e.g. for caching, redundancy or similar purposes), unless this is expressly allowed under the laws or regulations of the KSA. (Article 3.3.8)</p> <p>Public clouds Cloud Customers may not transfer, store or process Level 3 Customer Content to or in any public, community or hybrid cloud unless and for as long as the CSP is validly registered with the CITC. (Article 3.3.9)</p> <p>CSPs must inform their Cloud Customers in advance whether their Customer Content will be transferred, stored or processed outside the KSA, permanently or temporarily. (Article 3.3.11)</p>	
Security	<p>Classification Customer Content can be subject to different levels of information security, depending on the required level of preservation of the Customer Content's confidentiality, integrity and availability. (Article 3.3.1)</p> <p>Data sharing Cloud Customers are obliged to ensure that, if allowed, any outsourcing, transmission, Processing or storage should be subject to certain information security or data protection restrictions or safeguards, in addition to those specified to Cloud Framework. (Article 3.3.3.2)</p> <p>Security features CSPs must inform any Cloud Customer, upon his request, of the information security features offered by the CSP or applied to the Cloud Customer's Customer Content. CSPs may also satisfy this obligation by making such information available in online format for Cloud Customers. (Article 3.3.7)</p> <p>Information security Cloud Customers are responsible for:</p> <ul style="list-style-type: none"> • selecting the appropriate information security level which best matches their specific needs, duties, obligations and security requirements. (Article 3.3.5) • for implementing all information security features required for part or the whole of their Personal Data. (Article 3.3.6) 	

Cloud Framework		General Observations
	<p>Business continuity, disaster recovery, risk management</p> <p>Cloud Providers must adopt internal rules and policies on business continuity, disaster recovery and risk management, and provide to their Cloud Customers or the CSPs they co-operate with, upon their request, a summary of these rules and policies. (Article 3.3.15)</p>	
Administrative Fines and Regulatory Sanctions	<p>Violations</p> <p>Any violation of the Cloud Framework shall be subject to the penalties that the ICTs may impose under Commission Statutes, without prejudice to any penalties that may be imposed under any other applicable law in the KSA. (Article 3.10.1)</p> <p>Exclusion of liability</p> <p>CSPs may not contractually exclude their liability to their individual consumer Cloud Customers for any loss of, or damage to, inter alia, Cloud Customer Personal Data, if this is linked to the CSP's Processing of, or other interaction with, such Cloud Customer Personal Data if these may be reasonably attributed, in whole or in part, to intentional or negligent acts or omissions of those CSPs. (Article 3.7.2)</p>	
Role and Powers of the CITC	<p>Violations</p> <p>Any violation of the Cloud Framework shall be subject to the penalties that the ICTs may impose under Commission Statutes, without prejudice to any penalties that may be imposed under any other applicable law in the KSA. (Article 3.10.1)</p> <p>Guidance</p> <p>The CITC may issue guidelines, model Cloud Computing contracts or clauses, guides, recommendations or other texts aimed at:</p> <ul style="list-style-type: none"> clarifying any aspect of the present Regulatory Framework; providing guidance to CSPs, Cloud Customers and the public in general on any aspect of Cloud Computing; complementing the Cloud Framework through mandatory or voluntary detailed implementation provisions. (Article 3.10.2) 	

JORDAN



Jordan – Executive summary



This jurisdictional overview is based on an unofficial English translation of the draft Data Protection Bill issued in 2018. No English language version is currently available.

There is currently no specific data protection legislation in place in Jordan. The Jordanian Ministry of Communications (**MOC**) submitted a draft bill for data protection in 2014. In September 2018, the MOC called for a third public consultation on the draft law with reference to the GDPR. It is generally accepted that the latest draft still has major issues including:

- ensuring the independence of the Jordanian Privacy Commission (**JPC**), as the law proposes an assigned council for the JPC with majority of its members appointed from government;
- the draft law's lack of incorporation of international standards and best practices for the protection of Personal Data; and
- the lack of consideration for modern forms of Personal Data Processing.

For example, where a Data Subject withdraws their consent to Processing, the Data Controller has one month to comply with the revocation. In addition, unlike the GDPR (which requires organisations to notify Data Subjects of the purposes of the Processing, data to be processed etc. either at the time the information is collected or within a reasonable period thereafter), the draft law requires such information to be provided in advance of the Processing.

The draft bill appears broadly based on the GDPR, with the incorporation of the main concepts of transparency, accuracy, storage limitation and data minimisation. The draft law also stipulates, similar to the GDPR, that data

breaches be reported to the Personal Data Protection Board within 72 hours and to Data Subjects within 24 hours. There are also provisions governing the lawful bases for Processing, data security considerations and Data Subject rights. However, the draft bill seems more vague when compared with the GDPR and other data protection laws in the region – the bill does not fully flesh out Data Subject rights as the GDPR does and leaves several matters to be dealt with by specific regulations such as the conditions for the disclosure of Personal Data, the entities that are permitted to disclose the data and the Personal Data that is permitted to be disclosed.

While there is currently no overarching data protection law in Jordan, a number of provisions scattered across different statutes afford some protection to Personal Data and the confidentiality of private communications.

The *Constitution* contains a specific provision concerning privacy wherein it states that all postal and telegraphic correspondence, telephonic communications, and the other communications means are regarded as secret and shall not be subject to viewing except by a judicial order. The *Information Systems Crimes Law* (Law No 30 of 2010 on Information Systems Crimes) punishes unlawful surveillance or monitoring of communications sent using information systems or the internet. The *Penal Code* (Law No 16 of 1960) also penalises the dissemination of content of private messages.

GDPR		Information Systems Crimes Law	General Observations
Principles of Data Processing	Lawfulness, fairness, transparency Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. (Article 5(1)(a))	Lawful basis An individual's consent must be obtained in order to process their Personal Data including disclosing any obtained by such Processing.	Status There is currently no specific data protection legislation in place in Jordan. However, a draft bill for data protection was published in 2014 and revised in 2018 to reflect the GDPR. Notwithstanding, it is generally accepted that the latest draft still has major issues regarding ensuring the independence of the Jordanian Privacy Commission and with adhering to international standards for the protection of Personal Data.
	Specified purposes Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. (Article 5(1)(b))		
	Data minimisation Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. (Article 5(1)(c))		
	Accuracy Personal Data must be accurate and, where necessary, kept up to date. (Article 5(1)(d))		
	Storage limitation Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. (Article 5(1)(e))		
	Integrity and confidentiality Personal Data must be processed in a way 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. (Article 5(1)(f))		
	Accountability The controller shall be responsible for and be able to demonstrate compliance with all the above principles. (Article 5(2))		

GDPR		Information Systems Crimes Law	General Observations
	<p>Lawful bases The legal bases under which Personal Data may be processed are:</p> <ul style="list-style-type: none"> • with the freely given, specific, informed and unambiguous consent of the Data Subject; • where necessary for the performance of a contract to which the Data Subject is party; • where necessary to comply with a legal obligation to which the controller is subject; • where necessary to protect the vital interests of the Data Subject or another person; • where 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 • where necessary for the purposes of the legitimate interests of the controller or a third party. (Article 6(1)) 		
Data Controller and Data Processor Obligations	<p>General principles The controller is responsible for compliance with the principles listed in Article 5 (as set out above).</p> <p>The controller must have regard to 'data protection by design and by default' throughout their Processing activities.</p> <p>Lawful processing The controller must carry only process Personal Data under one of the conditions laid out in Article 6 and for special categories of Personal Data those laid out in Article 9.</p> <p>Sensitive personal data The Processing of sensitive Personal Data is prohibited, unless the:</p> <ul style="list-style-type: none"> • Data Subject has given explicit consent. (Article 9(2)(a)) • Processing is necessary in the context of employment law, or laws relating to social security and social protection. (Article 9(2)(b)) 	<p>Lawful basis An individual's consent must be obtained in order to process their Personal Data including disclosing any documents obtained by such Processing.</p>	<p>The GDPR places significantly more onerous burdens on Data Controllers and Data Processors than any law in Jordan.</p> <p>Data Processing agreements are not governed by any laws or regulations in Jordan. No standard form or precedent data Processing agreements have been approved by the national authorities or Jordanian courts.</p>

GDPR	Information Systems Crimes Law	General Observations
	<ul style="list-style-type: none"> • Processing is necessary to protect vital interests of the Data Subject (or another person). (Article 9(2)(c)) • Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim. (Article 9(2)(d)) • Processing relates to Personal Data which are manifestly made public by the Data Subject. (Article 9(2)(e)) • Processing is necessary for the establishment, exercise or defence of legal claims. (Article 9(2)(f)) • Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law. (Article 9(2)(g)) • Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional. (Article 9(2)(h)) • Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law. (Article 9(2)(i)) • Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. (Article 9(2)(j)) <p>Technical & organisational measures The controller is responsible for implementing appropriate technical and organisational measures to ensure and demonstrate that its Processing activities are compliant with the requirements of the GDPR. (Article 32)</p>	

GDPR	Information Systems Crimes Law	General Observations
<p>Data subject rights The controller must demonstrate the Data Subject's consent to Processing their Personal Data. The consent must be clearly presented and easily distinguished from other matters, in an intelligible and easily accessible form. The consent must be able to be withdrawn at any time. (Article 24)</p> <p>The controller must make reasonable efforts to verify parental consent (when the child is under 16, although in some members states may be as young as 13).</p> <p>Choosing a data processor The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of this Regulation and ensure the protection of the rights of the Data Subject.</p> <p>Processing by a processor shall be governed by a contract or other legal act. (Article 28)</p> <p>Notifications In the case of a Personal Data breach, the controller must notify the supervisory authority of the breach. This must be done without due delay and, where feasible, not later than 72 hours after having become aware of it. (Article 33)</p> <p>Record keeping Each controller must maintain a record of its Processing activities. (Article 30)</p> <p>Appoint a representative The controller must appoint an EU representative in certain situations. (Article 27)</p> <p>Appoint a DPO The controller must appoint a Data Protection Officer (DPO) in certain situations. (Article 37(1))</p>		

GDPR		Information Systems Crimes Law	General Observations
Data Subject Rights	Transparent communication In order to ensure that Personal Data are processed fairly and lawfully, controllers must provide certain minimum information to Data Subjects, regarding the collection and further Processing of their Personal Data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. (Articles 5(1)(a), 12-14)	No specific relevant provisions exist.	There is no general protection of Data Subject rights in line with the GDPR in Jordan. Shari'a principles, the Constitution and the Penal Code provide merely the right not to have their personal information captured without their consent and to have the confidentiality of such information maintained.
	Data subject rights Data controllers have a legal obligation to give effect to the rights of Data Subjects. (Article 12(2))		
	Identifying data subjects Data controllers must not refuse to give effect to the rights of a Data Subject unless the controller cannot identify the Data Subject. The controller must use all reasonable efforts to verify the identity of Data Subjects. Where the controller has reasonable doubts as to the identity of the Data Subject, the controller may request the provision of additional information necessary to confirm the identity of the Data Subject, but is not required to do so. (Article 12(2), (6))		
	Time limits A controller must, within one month of receiving a request made under those rights, provide any requested information in relation to any of the rights of Data Subjects. If the controller fails to meet this deadline, the Data Subject may complain to the relevant DPSA and may seek a judicial remedy. Where a controller receives large numbers of requests, or especially complex requests, the time limit may be extended by a maximum of two further months. (Article 12(3) - (4))		
	Basic Information Data Subjects have the right to be provided with information on the identity of the controller, the reasons for Processing their Personal Data and other relevant information necessary to ensure the fair and transparent Processing of Personal Data. (Articles 13 and 14)		

GDPR	Information Systems Crimes Law	General Observations
<p>Right of access Data Subjects have the right to obtain the following:</p> <ul style="list-style-type: none"> • confirmation of whether, and where, the controller is Processing their Personal Data; • information about the purposes of the Processing; • information about the categories of data being processed; • information about the categories of recipients with whom the data may be shared; • information about the period for which the data will be stored (or the criteria used to determine that period); • information about the existence of the rights to erasure, to rectification, to restriction of Processing and to object to Processing; • information about the existence of the right to complain to the DPSA; • where the data were not collected from the Data Subject, information as to the source of the data; and • information about the existence of, and an explanation of the logic involved in any automated Processing that has a significant effect on Data Subjects; and • Data Subjects may request a copy of the Personal Data being processed. (Article 15) <p>Access fees Data controllers must give effect to the rights of access, rectification, erasure and the right to object, free of charge. The controller may charge a reasonable fee for "repetitive requests", "manifestly unfounded or excessive requests" or "further copies". (Articles 12(5), 15(3), (4))</p> <p>Rectification Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data Subjects have the right to rectification of inaccurate Personal Data. (Articles 5(1)(d), 16)</p>		

GDPR	Information Systems Crimes Law	General Observations
<p>Erasure Data Subjects have the right to erasure of Personal Data if:</p> <ul style="list-style-type: none"> the data are no longer needed for their original purpose (and no new lawful purpose exists); the lawful basis for the Processing is the Data Subject's consent, the Data Subject withdraws that consent, and no other lawful ground exists; the Data Subject exercises the right to object, and the controller has no overriding grounds for continuing the Processing; the data have been processed unlawfully; or erasure is necessary for compliance with EU law or the national law of the relevant Member State. (Article 17) <p>Restrict processing Data Subjects have the right to restrict the Processing of Personal Data (meaning that the data may only be held by the controller, and may only be used for limited purposes) if:</p> <ul style="list-style-type: none"> the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); the Processing is unlawful and the Data Subject requests restriction (as opposed to exercising the right to erasure); the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or if verification of overriding grounds is pending, in the context of an erasure request. (Article 18) <p>Portability Data Subjects have a right to:</p> <ul style="list-style-type: none"> receive a copy of their Personal Data in a structured, commonly used, machine-readable format that supports re-use; 		

GDPR	Information Systems Crimes Law	General Observations
<ul style="list-style-type: none"> • transfer their Personal Data from one controller to another; • store their Personal Data for further personal use on a private device; and • have their Personal Data transmitted directly between controllers without hindrance. (Article 20) <p>Object to processing Data Subjects have the right to object, on grounds relating to their particular situation, to the Processing of Personal Data, where the basis for that Processing is either:</p> <ul style="list-style-type: none"> • public interest; or • legitimate interests of the controller. <p>The controller must cease such Processing unless the controller:</p> <ul style="list-style-type: none"> • demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject; or • requires the data in order to establish, exercise or defend legal rights. (Article 21) <p>Where Personal Data are processed for scientific and historical research purposes or statistical purposes, the Data Subject has the right to object, unless the Processing is necessary for the performance of a task carried out for reasons of public interest. (Articles 21(6), 83(1))</p> <p>Object to direct marketing Data Subjects have the right to object to the Processing of Personal Data for the purpose of direct marketing, including profiling. (Article 21(2) – (3))</p> <p>Duty to inform of right to object The right to object to Processing of Personal Data noted above must be communicated to the Data Subject no later than the time of the first communication with the Data Subject.</p>		

GDPR	Information Systems Crimes Law	General Observations
	<p>This information should be provided clearly and separately from any other information provided to the Data Subject. (Articles 3(2)(b), 14(2)(c), 15(1)(e), 21(4))</p> <p>Automated processing Data Subjects have the right not to be subject to a decision based solely on automated Processing which significantly affect them (including profiling). Such Processing is permitted where:</p> <ul style="list-style-type: none"> • it is necessary for entering into or performing a contract with the Data Subject provided that appropriate safeguards are in place; • it is authorised by law; or • the Data Subject has explicitly consented and appropriate safeguards are in place. (Article 22) 	
<p>Cross-Border Transfer Rules</p>	<p>General prohibition Cross-Border Personal Data Transfers may only take place if the transfer is made to an Adequate Jurisdiction or the data exporter has implemented a lawful data transfer mechanism (or an exemption or derogation applies). (Articles 44, 45)</p> <p>Adequacy decisions Cross-border data transfers may take place if the third country receives an Adequacy Decision from the EU Commission. (Articles 44, 45)</p> <p>The EU Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the USA (subject to compliance with the terms of the US-EU PrivacyShield).</p> <p>Public authorities Cross-border data transfers between public authorities may take place under agreements between public authorities, which do not require any specific authorisation from a DPSA. (Articles 46(2)(a), 46(3)(b))</p>	<p>No specific relevant provisions exist.</p> <p>There is no regulation currently dealing with the transfer of data outside Jordan. Data transfer agreements are not governed by any laws or regulations in Jordan. No standard form or precedent data transfer agreements have been approved by the national authorities or Jordanian courts.</p> <p>NOTE: Under the GDPR, Cross-border data transfers may take place on the basis of standard data protection clauses approved by the EU Commission (“Model Clauses”). The current set of Model Clauses are currently being challenged as a form of appropriate data transfer mechanism; therefore their future is uncertain. In January 2019, the Irish Supreme Court (as part of the <i>Schrems v Facebook</i> litigation) heard an appeal by Facebook over a decision of the Irish High Court to refer a number of questions to the Court of Justice of the EU (“CJEU”) regarding the validity of this data transfer mechanism. The Supreme Court will publish its decision in due course. If Facebook is unsuccessful in its appeal, the CJEU will rule on these questions, which may result in a declaration that the Model Clauses are no longer valid as a transfer mechanism.</p>

GDPR	Information Systems Crimes Law	General Observations
<p>Binding Corporate Rules Cross-Border Transfer within a corporate group may take place on the basis of Binding Corporate Rules ("BCRs"). BCRs require approval from DPSAs, but approved, individual transfers made under the BCRs do not require further approval. (Articles 4(20) 46(2)(b), 47)</p> <p>Model clauses Cross-border data transfers may take place on the basis of the Model Clauses entered into between the data exporter and data recipient. Existing Model Clauses implemented under the 1995 Directive remain valid until amended, replaced or repealed under the GDPR. (Articles 28(6)-(8), 46(2)(c), 57(1)(j), (r), 93(2))</p> <p>Other mechanisms Cross-border data transfers may take place on the basis, <i>inter alia</i>, of:</p> <ul style="list-style-type: none"> • standard data protection clauses adopted by one or more DPSAs under the GDPR. (Articles 46(2)(d), 64(1)(d), 57(1)(j), (r), 93(2)) • an approved code of conduct, together with binding and enforceable commitments to provide appropriate safeguards. (Articles 40, 41, 46(2)(e)) • certifications together with binding and enforceable commitments of the data importer to apply the certification to the transferred data. (Articles 42, 43, 46(2)(f)) • ad hoc clauses conforming to the GDPR and approved by the relevant DPSA. (Articles 46(3)(a), (4), 63)) • administrative arrangements between public authorities (e.g., MOUs) subject DPSA approval. (Articles 46(3)(b), (4), 63) <p>Derogations Cross-border data transfers may be made on the basis, <i>inter alia</i>, that:</p> <ul style="list-style-type: none"> • the Data Subject explicitly consents having been informed of the possible risks of such transfer. (Article 49(1)(a), (3)) 		

GDPR		Information Systems Crimes Law	General Observations
	<ul style="list-style-type: none"> the performance of a contract between the Data Subject and the controller. (Article 49(1)(b), (3)) it is necessary for the purposes of performing or concluding a contract in the interests of the Data Subject. (Article 49(1)(c), (3)) the transfer is necessary for important reasons of public interest. (Article 49(1)(d), (4)) it is necessary for the purposes of legal proceedings, or obtaining legal advice. (Article 49(1)(e)) the transfer is necessary in order to protect the vital interests of the Data Subject, where the Data Subject is incapable of giving consent. (Article 49(1)(f)) the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by those of the individual subject to informing the relevant DPSA and the Data Subjects. (Article 49(1), (3), (6)) 		
Personal Data Security	<p>Security Data controllers must implement appropriate technical and organisational security measures to protect Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.</p> <p>Depending on the nature of the Processing, these measures may include:</p> <ul style="list-style-type: none"> encryption of the Personal Data; on-going reviews of security measures; redundancy and back-up facilities; and regular security testing. (Article 32) 	No specific relevant provisions exist.	There are no specific provisions relating to Personal Data security outside the requirement of general principles of law to keep such data confidential.
Administrative Fines and Regulatory Sanctions	<p>Judicial remedies Data Subjects have the right to an effective judicial remedy against:</p> <ul style="list-style-type: none"> decisions of a DPSA concerning them; any failure by a DPSA to deal with, or respond to, a complaint within three months; and 	<p>Deletion of personal data Anyone who intentionally and without authorisation accesses a website or informational system with the purpose of cancelling, deleting, adding, destroying, disclosing, extinguishing, blocking, altering, changing, transferring or copying data or information or assuming the identity of its owner, shall be subject to:</p>	<p>The absence of a national DPSA means that there is no effective supervision and/or enforcement of Data Subject rights or data protection principles in Jordan.</p> <p>Cybercrime is severely punished under the Information Systems Crimes Law and penalties are imposed for identity theft, defamation, electronic piracy, email theft and other unlawful activities.</p>

GDPR	Information Systems Crimes Law	General Observations
<ul style="list-style-type: none"> any unlawful Processing of their Personal Data by a controller or processor. (Article 78-79) <p>Compensation & liability A Data Subject who has suffered harm as a result of the unlawful Processing of his or her Personal Data has the right to receive compensation from the controller or processor for the harm suffered:</p> <ul style="list-style-type: none"> Any controller involved in the Processing is liable for the harm caused. A processor is liable for the harm caused by any of its (or its sub-processor's) Processing activities that are not in compliance with its obligations under the GDPR, or are in breach of the controller's instructions. To ensure effective compensation, each controller or processor will be held liable for the entirety of the harm caused, if they are involved in the same Processing and responsible for that harm. (Article 82(1)-(2), (4)) <p>Joint-controller liability Data Subjects are entitled to enforce their rights against any of the joint controllers. Each joint controller is liable for the entirety of the damage, although national law may apportion liability between them. If one joint controller has paid full compensation, it may then bring proceedings against the other joint controllers to recover their portions of the damages. (Article 26(3), 82(3)-(5))</p> <p>Exemptions from liability A controller or processor is exempt from liability if it proves that it is not responsible for the event giving rise to the harm. There is no mention of force majeure events. (Article 82(3))</p> <p>Administrative fines The maximum fine that can be imposed for serious infringements of the GDPR is the greater of €20 million or 4% of an undertaking's worldwide turnover for the preceding financial year. (Article 83(5) – (6))</p>	<ul style="list-style-type: none"> imprisonment for a period between 3 months and 1 year; and/or a fine not exceeding 1,000 Dinars. (Article 3) <p>Misuse of computer programs Any person who installs, publishes or uses intentionally a program through an information network or information system without consent with the purpose of cancelling, deleting, adding, destroying, disclosing, extinguishing, blocking, altering, changing, transferring, copying, capturing, or enabling others to view data or information, or assuming the identity of the owner shall be subject to:</p> <ul style="list-style-type: none"> imprisonment for a period between 3 months and 1 year; and/or a fine between 200 – 1,000 Dinars. (Article 4) <p>Interception Anyone who intentionally captures, interferes or intercepts data or information transmitted through an information network or any information system shall be subject to:</p> <ul style="list-style-type: none"> imprisonment for a period between 1 month and 1 year; and/or a fine between 200 – 1,000 Dinars. (Article 5) <p>Credit card data Anyone who intentionally and without authorisation obtains through an information network or any information system data or information relating to credit cards or data or information that is used in execution of electronic financial or banking transactions shall be subject to:</p> <ul style="list-style-type: none"> imprisonment for a period between 3 months and 2 years; and/or a fine between 500 – 2,000 Dinars. (Article 6(A)) 	

	GDPR	Information Systems Crimes Law	General Observations
	<p>Fine criteria When deciding whether to impose a fine and deciding on the amount, DPSAs are required to give due regard to a range of issues, including:</p> <ul style="list-style-type: none"> the nature, gravity and duration of the infringement; the number of Data Subjects affected and the level of harm suffered by them; the intentional or negligent character of the infringement; any action taken by the controller or processor to mitigate the harm; any relevant previous infringements by the controller or processor; the degree of co-operation with the relevant DPSA; whether the infringement was self-reported by the controller or processor; and any other aggravating or mitigating factors. (Article 82(3)) 	<p>Anyone who intentionally uses through an information network or any information system data or banking transactions to obtain to oneself or others the data, information, assets or services of others shall be subject to:</p> <ul style="list-style-type: none"> imprisonment for not less than 1 year; and/or a fine between 1,000 – 5,000 Dinars. (Article 6(B)) <p>Offences during employment Punishments for the crimes in Articles 3 - 6 shall be doubled where committed during the performance of employment or work or by exploiting either one of them. (Article 7)</p>	
<p>Role and Powers of any relevant Data Protection Supervisory Authority</p>	<p>Independence DPSAs must act independently and operate free from all outside influences, including government control. (Article 52)</p> <p>Tasks The tasks of DPSAs include obligations to:</p> <ul style="list-style-type: none"> monitor and enforce the application of the GDPR; promote awareness of the risks, rules, safeguards and rights pertaining to Personal Data (especially in relation to children); advise national and governmental institutions on the application of the GDPR; hear claims brought by Data Subjects or their representatives, and inform Data Subjects of the outcome of such claims; establish requirements for Impact Assessments; encourage the creation of Codes of Conduct and review certifications; authorise Model Clauses and BCRs; 	<p>No specific relevant provisions exist.</p>	<p>The absence of a national DPSA means that there is no effective supervision and/or enforcement of Data Subject rights or data protection principles in Jordan.</p>

GDPR		Information Systems Crimes Law	General Observations
	<ul style="list-style-type: none"> • keep records of sanctions and enforcement actions; and • fulfil "any other tasks related to protection of Personal Data". (Article 55, 57) <p>Powers DPSAs are empowered to oversee enforcement of the GDPR, investigate breaches of the GDPR and bring legal proceedings where necessary. (Article 58)</p>		

KUWAIT



Kuwait – Executive summary



There is currently no specific data protection legislation in place in Kuwait. There are no clear legal guidelines to determine how and when Personal Data may be collected, stored, transferred, used, or otherwise Processed.

The *Kuwaiti Constitution* places broad restrictions on the disclosure of the contents of communications unless permitted by law.

The closest law in Kuwait to a data protection law is the *E-Transactions Law* (Law No. 20 of 2014). This law requires that the recipient of client data and its employees must retain client data relating to positional affairs, personal status,

health status, certain financial information and other personal information, privately and confidentially. The law also states that client consent is required for the disclosure of their data.

The *Cybercrime Law* (Law No 63 of 2015) protects data and information and specifies penalties of imprisonment and fines for violations.

It is not known whether Kuwait will introduce and implement a specific data protection law. However, given the regional shift towards protecting Personal Data and the global reach of the GDPR, it would be considered likely that such a law will be implemented in the near future

	GDPR	E-Transactions Law	Cybercrime Law	General Observations
Principles of Data Processing	<p>Lawfulness, fairness, transparency Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. (Article 5(1)(a))</p> <p>Specified purposes Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. (Article 5(1)(b))</p> <p>Data minimisation Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. (Article 5(1)(c))</p> <p>Accuracy Personal Data must be accurate and, where necessary, kept up to date. (Article 5(1)(d))</p> <p>Storage limitation Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. (Article 5(1)(e))</p> <p>Integrity and confidentiality Personal Data must be processed in a way 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. (Article 5(1)(f))</p>	<p>Definition The law does not define Personal Data, but it is considered to include at least personal information about positional affairs, personal status, health status and information regarding financial disclosures.</p> <p>General obligation 'Institutions' (governmental bodies, agencies, public institutions, companies, non-governmental bodies or employees thereof) are generally prohibited from collecting or Processing any information in an illegal manner, except with the consent of the person concerned or their representative. (Articles 32, 35)</p> <p>Specified purposes The 'institutions' must state the purpose of collecting the data and the collection must be carried out within the limits of this purpose.</p> <p>The 'institutions' must not use the data for purposes other than those for which it was collected. (Article 35)</p> <p>Accuracy The accuracy of personal information must be verified and must be updated regularly. (Article 35)</p>	<p>Lawful basis An individual's consent must be obtained in order to process their Personal Data including disclosing any obtained by such Processing.</p>	<p>Status Kuwait does not yet have a specific Personal Data protection law. The closest law it does have to a data protection law, is the E-Transactions Law. This law requires that the recipient and its employees must retain client data relating to positional affairs, personal status, health status, certain financial information and other personal information privately and confidentially. The law also states that client consent is required for the disclosure of their data.</p> <p>Looking forward At this moment in time, there is no known plans to implement a specific data protection law in Kuwait. However, it seems likely that such a law will be implemented in the near future following recent trends from other jurisdictions in the region.</p>

GDPR		E-Transactions Law	Cybercrime Law	General Observations
	<p>Accountability The controller shall be responsible for and be able to demonstrate compliance with all the above principles. (Article 5(2))</p> <p>Lawful bases The legal bases under which Personal Data may be processed are</p> <ul style="list-style-type: none"> • with the freely given, specific, informed and unambiguous consent of the Data Subject; • where necessary for the performance of a contract to which the Data Subject is party; • where necessary to comply with a legal obligation to which the controller is subject; • where necessary to protect the vital interests of the Data Subject or another person; • where 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 • where necessary for the purposes of the legitimate interests of the controller or a third party. (Article 6(1)) 			
Data Controller and Data Processor Obligations	<p>General principles The controller is responsible for compliance with the principles listed in Article 5 (as set out above).</p> <p>The controller must have regard to 'data protection by design and by default' throughout their Processing activities.</p>	<p>There is no concept of 'data controller' or 'data processor' or similar in this law.</p> <p>Lawful basis An individual's consent must be obtained in order to process their Personal Data including disclosing any documents obtained by such Processing.</p>	<p>Lawful basis An individual's consent must be obtained in order to process their Personal Data including disclosing any documents obtained by such Processing.</p>	<p>The GDPR places significantly more onerous burdens on Data Controllers and Data Processors than any law in Kuwait.</p> <p>Data Processing agreements are not governed by any laws or regulations in Kuwait. No standard form or precedent data Processing agreements have been approved by the national authorities or Kuwaiti courts.</p>

GDPR	E-Transactions Law	Cybercrime Law	General Observations
<p>Lawful processing The controller must carry only process Personal Data under one of the conditions laid out in Article 6 and for special categories of Personal Data those laid out in Article 9.</p> <p>Sensitive personal data he Processing of sensitive Personal Data is prohibited, unless the:</p> <ul style="list-style-type: none"> • Data Subject has given explicit consent. (Article 9(2)(a)) • Processing is necessary in the context of employment law, or laws relating to social security and social protection. (Article 9(2)(b)) • Processing is necessary to protect vital interests of the Data Subject (or another person). (Article 9(2)(c)) • Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim. (Article 9(2)(d)) • Processing relates to Personal Data which are manifestly made public by the Data Subject. (Article 9(2)(e)) • Processing is necessary for the establishment, exercise or defence of legal claims. (Article 9(2)(f)) • Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law. (Article 9(2)(g)) • Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of 			

GDPR	E-Transactions Law	Cybercrime Law	General Observations
	<p>the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional. (Article 9(2)(h))</p> <ul style="list-style-type: none"> Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law. (Article 9(2)(i)) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. (Article 9(2)(j)) <p>Technical & organisational measures The controller is responsible for implementing appropriate technical and organisational measures to ensure and demonstrate that its Processing activities are compliant with the requirements of the GDPR. (Article 32)</p> <p>Data subject rights The controller must demonstrate the Data Subject's consent to Processing their Personal Data. The consent must be clearly presented and easily distinguished from other matters, in an intelligible and easily accessible form. The consent must be able to be withdrawn at any time. (Article 24)</p>		

GDPR	E-Transactions Law	Cybercrime Law	General Observations
<p>The controller must make reasonable efforts to verify parental consent (when the child is under 16, although in some members states may be as young as 13).</p> <p>Choosing a data processor The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of this Regulation and ensure the protection of the rights of the Data Subject.</p> <p>Processing by a processor shall be governed by a contract or other legal act. (Article 28)</p> <p>Notifications In the case of a Personal Data breach, the controller must notify the supervisory authority of the breach. This must be done without due delay and, where feasible, not later than 72 hours after having become aware of it. (Article 33)</p> <p>Record keeping Each controller must maintain a record of its Processing activities. (Article 30)</p> <p>Appoint a representative The controller must appoint an EU representative in certain situations. (Article 27)</p> <p>Appoint a DPO The controller must appoint a Data Protection Officer (DPO) in certain situations. (Article 37(1))</p>			

	GDPR	E-Transactions Law	Cybercrime Law	General Observations
Data Subject Rights	<p>Transparent communication In order to ensure that Personal Data are processed fairly and lawfully, controllers must provide certain minimum information to Data Subjects, regarding the collection and further Processing of their Personal Data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. (Articles 5(1)(a), 12-14)</p> <p>Data subject rights Data controllers have a legal obligation to give effect to the rights of Data Subjects. (Article 12(2))</p> <p>Identifying data subjects Data controllers must not refuse to give effect to the rights of a Data Subject unless the controller cannot identify the Data Subject. The controller must use all reasonable efforts to verify the identity of Data Subjects. Where the controller has reasonable doubts as to the identity of the Data Subject, the controller may request the provision of additional information necessary to confirm the identity of the Data Subject, but is not required to do so. (Article 12(2), (6))</p> <p>Time limits A controller must, within one month of receiving a request made under those rights, provide any requested information in relation to any of the rights of Data Subjects. If the controller fails to meet this deadline, the Data Subject may complain to the relevant DPSA and may seek a judicial remedy. Where a controller receives large numbers of requests, or especially complex requests, the time limit</p>	<p>Right to access Except from where for purposes of national security, individuals may request access to the Personal Data or information registered about them. (Article 33)</p> <p>Right to request/receive a copy Except from where for purposes of national security, individuals may also make a request to obtain a formal extract of their data. (Article 34)</p> <p>Right to deletion Individuals have the right to request the 'institutions' to delete or amend any of their Personal Data or information which are kept in the records or electronic Processing systems, if they are invalid or untrue. (Article 36)</p>	No specific relevant provisions exist.	There are very limited measures in place under Kuwait law to enable Data Subjects to vindicate their rights with no general protection of Data Subject rights in line with the GDPR. The E-Transactions Law provides certain basic rights of access and deletion.

GDPR	E-Transactions Law	Cybercrime Law	General Observations
<p>may be extended by a maximum of two further months. (Article 12(3) - (4))</p> <p>Basic information Data Subjects have the right to be provided with information on the identity of the controller, the reasons for Processing their Personal Data and other relevant information necessary to ensure the fair and transparent Processing of Personal Data. (Articles 13 and 14)</p> <p>Right of access Data Subjects have the right to obtain the following:</p> <ul style="list-style-type: none"> • confirmation of whether, and where, the controller is Processing their Personal Data; • information about the purposes of the Processing; • information about the categories of data being processed; • information about the categories of recipients with whom the data may be shared; • information about the period for which the data will be stored (or the criteria used to determine that period); • information about the existence of the rights to erasure, to rectification, to restriction of Processing and to object to Processing; • information about the existence of the right to complain to the DPSA; • where the data were not collected from the Data Subject, information as to the source of the data; and • information about the existence of, and an explanation of the logic involved in 			

GDPR	E-Transactions Law	Cybercrime Law	General Observations
<p>any automated Processing that has a significant effect on Data Subjects; and</p> <ul style="list-style-type: none"> Data Subjects may request a copy of the Personal Data being processed. (Article 15) <p>Access fees Data controllers must give effect to the rights of access, rectification, erasure and the right to object, free of charge. The controller may charge a reasonable fee for "repetitive requests", "manifestly unfounded or excessive requests" or "further copies". (Articles 12(5), 15(3), (4))</p> <p>Rectification Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data Subjects have the right to rectification of inaccurate Personal Data. (Articles 5(1)(d), 16)</p> <p>Erasure Data Subjects have the right to erasure of Personal Data if:</p> <ul style="list-style-type: none"> the data are no longer needed for their original purpose (and no new lawful purpose exists); the lawful basis for the Processing is the Data Subject's consent, the Data Subject withdraws that consent, and no other lawful ground exists; the Data Subject exercises the right to object, and the controller has no overriding grounds for continuing the Processing; the data have been processed unlawfully; or 			

GDPR	E-Transactions Law	Cybercrime Law	General Observations
<ul style="list-style-type: none"> • erasure is necessary for compliance with EU law or the national law of the relevant Member State. (Article 17) <p>Restrict processing Data Subjects have the right to restrict the Processing of Personal Data (meaning that the data may only be held by the controller, and may only be used for limited purposes) if:</p> <ul style="list-style-type: none"> • the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); • the Processing is unlawful and the Data Subject requests restriction (as opposed to exercising the right to erasure); • the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or • if verification of overriding grounds is pending, in the context of an erasure request. (Article 18) <p>Portability Data Subjects have a right to:</p> <ul style="list-style-type: none"> • receive a copy of their Personal Data in a structured, commonly used, machine-readable format that supports re-use; • transfer their Personal Data from one controller to another; • store their Personal Data for further personal use on a private device; and • have their Personal Data transmitted directly between controllers without hindrance. (Article 20) 			

GDPR	E-Transactions Law	Cybercrime Law	General Observations
<p>Object to processing Data Subjects have the right to object, on grounds relating to their particular situation, to the Processing of Personal Data, where the basis for that Processing is either:</p> <ul style="list-style-type: none"> • public interest; or • legitimate interests of the controller. <p>The controller must cease such Processing unless the controller:</p> <ul style="list-style-type: none"> • demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject; or • requires the data in order to establish, exercise or defend legal rights. (Article 21) <p>Where Personal Data are processed for scientific and historical research purposes or statistical purposes, the Data Subject has the right to object, unless the Processing is necessary for the performance of a task carried out for reasons of public interest. (Articles 21(6), 83(1))</p> <p>Object to direct marketing Data Subjects have the right to object to the Processing of Personal Data for the purpose of direct marketing, including profiling. (Article 21(2) – (3))</p> <p>Duty to inform of right to object The right to object to Processing of Personal Data noted above must be communicated to the Data Subject no later than the time of the first communication with the Data Subject.</p>			

GDPR		E-Transactions Law	Cybercrime Law	General Observations
	<p>This information should be provided clearly and separately from any other information provided to the Data Subject. (Articles 3(2)(b), 14(2)(c), 15(1)(e), 21(4))</p> <p>Automated processing Data Subjects have the right not to be subject to a decision based solely on automated Processing which significantly affect them (including profiling). Such Processing is permitted where:</p> <ul style="list-style-type: none"> • it is necessary for entering into or performing a contract with the Data Subject provided that appropriate safeguards are in place; • it is authorised by law; or • the Data Subject has explicitly consented and appropriate safeguards are in place. (Article 22) 			
Cross-Border Transfer Rules	<p>General prohibition Cross-Border Personal Data Transfers may only take place if the transfer is made to an Adequate Jurisdiction or the data exporter has implemented a lawful data transfer mechanism (or an exemption or derogation applies). (Articles 44, 45)</p> <p>Adequacy decisions Cross-border data transfers may take place if the third country receives an Adequacy Decision from the EU Commission. (Articles 44, 45)</p> <p>The EU Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the</p>	<p>General prohibition It is illegal to transfer any personal information to another party without the consent of the person concerned or their representative. (Article 32)</p>	No specific relevant provisions exist.	<p>There is no regulation currently dealing specifically with the transfer of data outside Kuwait. Data transfer agreements are not governed by any laws or regulations in Kuwait. No standard form or precedent data transfer agreements have been approved by the national authorities or Kuwaiti courts.</p> <p>NOTE: Under the GDPR, Cross-border data transfers may take place on the basis of standard data protection clauses approved by the EU Commission ("Model Clauses"). The current set of Model Clauses are currently being challenged as a form of appropriate data transfer mechanism; therefore their future is uncertain.</p>

GDPR	E-Transactions Law	Cybercrime Law	General Observations
<p>USA (subject to compliance with the terms of the US-EU Privacy Shield).</p> <p>Public authorities Cross-border data transfers between public authorities may take place under agreements between public authorities, which do not require any specific authorisation from a DPSA. (Articles 46(2)(a), 46(3)(b))</p> <p>Binding Corporate Rules Cross-Border Transfer within a corporate group may take place on the basis of Binding Corporate Rules ("BCRs"). BCRs require approval from DPSAs, but approved, individual transfers made under the BCRs do not require further approval. (Articles 4(20) 46(2)(b), 47)</p> <p>Model clauses Cross-border data transfers may take place on the basis of the Model Clauses entered into between the data exporter and data recipient. Existing Model Clauses implemented under the 1995 Directive remain valid until amended, replaced or repealed under the GDPR. (Articles 28(6)-(8), 46(2)(c), 57(1)(j), (r), 93(2))</p> <p>Other mechanisms Cross-border data transfers may take place on the basis, <i>inter alia</i>, of:</p> <ul style="list-style-type: none"> • standard data protection clauses adopted by one or more DPSAs under the GDPR. (Articles 46(2)(d), 64(1)(d), 57(1)(j), (r), 93(2)) • an approved code of conduct, together with binding and enforceable commitments to provide appropriate safeguards. (Articles 40, 41, 46(2)(e)) 			<p>In January 2019, the Irish Supreme Court (as part of the <i>Schrems v Facebook</i> litigation) heard an appeal by Facebook over a decision of the Irish High Court to refer a number of questions to the Court of Justice of the EU ("CJEU") regarding the validity of this data transfer mechanism. The Supreme Court will publish its decision in due course. If Facebook is unsuccessful in its appeal, the CJEU will rule on these questions, which may result in a declaration that the Model Clauses are no longer valid as a transfer mechanism.</p>

GDPR	E-Transactions Law	Cybercrime Law	General Observations
<ul style="list-style-type: none"> • certifications together with binding and enforceable commitments of the data importer to apply the certification to the transferred data. (Articles 42, 43, 46(2)(f)) • ad hoc clauses conforming to the GDPR and approved by the relevant DPSA. (Articles 46(3)(a), (4), 63)) • administrative arrangements between public authorities (e.g., MOUs) subject DPSA approval. (Articles 46(3)(b), (4), 63) <p>Derogations Cross-border data transfers may be made on the basis, <i>inter alia</i>, that:</p> <ul style="list-style-type: none"> • the Data Subject explicitly consents having been informed of the possible risks of such transfer. (Article 49(1)(a), (3)) • the performance of a contract between the Data Subject and the controller. (Article 49(1)(b), (3)) • it is necessary for the purposes of performing or concluding a contract in the interests of the Data Subject. (Article 49(1)(c), (3)) • the transfer is necessary for important reasons of public interest. (Article 49(1)(d), (4)) • it is necessary for the purposes of legal proceedings, or obtaining legal advice. (Article 49(1)(e)) • the transfer is necessary in order to protect the vital interests of the Data Subject, where the Data Subject is incapable of giving consent. (Article 49(1)(f)) • the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by those of the individual subject to informing the 			

GDPR		E-Transactions Law	Cybercrime Law	General Observations
	relevant DPSA and the Data Subjects. (Article 49(1), (3), (6))			
Personal Data Security	<p>Security Data controllers must implement appropriate technical and organisational security measures to protect Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.</p> <p>Depending on the nature of the Processing, these measures may include:</p> <ul style="list-style-type: none"> • encryption of the Personal Data; • on-going reviews of security measures; • redundancy and back-up facilities; and • regular security testing. (Article 32) 	<p>General measures The 'institutions' shall take appropriate measures to protect the Personal Data and information against loss, damage, disclosure, replacement with incorrect data or information, or addition of untrue information thereto. (Article 35)</p>	No specific relevant provisions exist.	There are no specific provisions relating to Personal Data security akin to the GDPR outside the requirement to take appropriate measures to protect the Personal Data and information against loss, damage, disclosure, replacement with incorrect data or information, or addition of untrue information thereto under the E-Transactions Law. This law provides no guidance on what may be included in "appropriate measures".
Administrative Fines and Regulatory Sanctions	<p>Judicial remedies Data Subjects have the right to an effective judicial remedy against:</p> <ul style="list-style-type: none"> • decisions of a DPSA concerning them; • any failure by a DPSA to deal with, or respond to, a complaint within three months; and • any unlawful Processing of their Personal Data by a controller or processor. (Article 78-79) <p>Compensation & liability A Data Subject who has suffered harm as a result of the unlawful Processing of his or her Personal Data has the right to receive compensation from the controller or processor for the harm suffered:</p>	<p>Fines Anyone who discloses personal information without proper consent or a court order shall be subject to a fine of no less than 5,000 Dinars. (Article 37)</p> <p>Imprisonment Violations of the law are also punishable by a maximum of 3 years imprisonment. (Article 37)</p> <p>Confiscation The law also provides for confiscation of tools, programs or devices that are used for unauthorised disclosure. (Article 37(F))</p>	<p>Unauthorised access Whoever commits unauthorised access to a computer, a computer system, an electronic data Processing system, an automated electronic system or an information network that results in the cancellation, deletion, damage, destruction, disclosure, alteration or re-publishing of Personal Data or information shall be subject to:</p> <ul style="list-style-type: none"> • imprisonment for a term not exceeding 3 years and/or • a fine not exceeding 10,000 Dinars. (Article 2) <p>Where this offence is committed by a person in the performance of their job, the penalty shall be:</p> <ul style="list-style-type: none"> • imprisonment for a term not exceeding 5 years and/or 	<p>The absence of a national DPSA means that there is no effective supervision and/or enforcement of Data Subject rights or data protection principles in Kuwait.</p> <p>Cybercrime is severely punished by the Kuwait Public Prosecution and penalties are imposed for identity theft, breaching confidentiality, stealing medical data, electronic piracy, email theft and other unlawful activities.</p>

GDPR	E-Transactions Law	Cybercrime Law	General Observations
<ul style="list-style-type: none"> Any controller involved in the Processing is liable for the harm caused. A processor is liable for the harm caused by any of its (or its sub-processor's) Processing activities that are not in compliance with its obligations under the GDPR, or are in breach of the controller's instructions. To ensure effective compensation, each controller or processor will be held liable for the entirety of the harm caused, if they are involved in the same Processing and responsible for that harm. (Article 82(1)-(2), (4)) <p>Joint-controller liability Data Subjects are entitled to enforce their rights against any of the joint controllers. Each joint controller is liable for the entirety of the damage, although national law may apportion liability between them. If one joint controller has paid full compensation, it may then bring proceedings against the other joint controllers to recover their portions of the damages. (Article 26(3), 82(3)-(5))</p> <p>Exemptions from liability A controller or processor is exempt from liability if it proves that it is not responsible for the event giving rise to the harm. There is no mention of force majeure events. (Article 82(3))</p> <p>Administrative fines The maximum fine that can be imposed for serious infringements of the GDPR is the greater of €20 million or 4% of an undertaking's worldwide turnover for the preceding financial year. (Article 83(5) – (6))</p>		<ul style="list-style-type: none"> a fine not exceeding 20,000 Dinars. (Article 2) <p>Confidential data Anyone who gains unauthorised access, directly, via the Internet or one of the information technology means, to a website or an information system with the purpose of obtaining government data, information considered confidential ipso jure, or data and information relating to the accounts of bank customers that results in the cancellation, damage, destruction, re-publishing or alteration of such data or information shall be subject to:</p> <ul style="list-style-type: none"> imprisonment for a term not exceeding 10 years and/or a fine between 5,000 - 20,000 Dinars. (Article 3(1)) <p>Medical data Anyone who deliberately alters or destroys, through the use of the Internet or an information technology means, an electronic document related to medical examinations, medical diagnosis, medical treatment, or medical care, or facilitates or enables others to commit such offence shall be subject to:</p> <ul style="list-style-type: none"> imprisonment for a term not exceeding 3 years and/or a fine between 3,000 - 10,000 Dinars. (Article 3(3)) <p>Interception Anyone who illegally eavesdrops, intercepts or receives data sent via the Internet or an information technology means shall be subject to:</p>	

GDPR		E-Transactions Law	Cybercrime Law	General Observations
	<p>Fine criteria When deciding whether to impose a fine and deciding on the amount, DPSAs are required to give due regard to a range of issues, including:</p> <ul style="list-style-type: none"> the nature, gravity and duration of the infringement; the number of Data Subjects affected and the level of harm suffered by them; the intentional or negligent character of the infringement; any action taken by the controller or processor to mitigate the harm; any relevant previous infringements by the controller or processor; the degree of co-operation with the relevant DPSA; whether the infringement was self-reported by the controller or processor; and any other aggravating or mitigating factors. (Article 82(3)) 		<ul style="list-style-type: none"> imprisonment for a term not exceeding 2 years and/or a fine between 2,000 - 5,000 Dinars. (Article 4) <p>Credit card data Anyone who uses the Internet or an information technology means to illegally gain access to figures, credit card data or the like shall be subject to:</p> <ul style="list-style-type: none"> imprisonment for a term not exceeding 1 year and/or a fine between 1,000 - 3,000 Dinars. (Article 5) <p>Confiscation A court may order that devices, programs and means, or the money earned by them, used to commit any of the crimes stipulated in this law be confiscated. (Article 13)</p> <p>Closure A court may rule that the shop or the place where any of these crimes were committed, with the knowledge of its owner, be closed for a period not exceeding one year, as the case may be, without prejudice to bona fide rights of others or the right of the aggrieved party to an appropriate compensation. (Article 13)</p>	
Role and Powers of any relevant Data Protection Supervisory Authority	<p>Independence DPSAs must act independently and operate free from all outside influences, including government control. (Article 52)</p> <p>Tasks The tasks of DPSAs include obligations to:</p>	There is no Data Protection Supervisory Authority or equivalent.	The Public Prosecution has sole responsibility to investigate, prosecute and plead in all crimes under this law.	The absence of a national DPSA means that there is no effective supervision and/or enforcement of Data Subject rights or data protection principles in Kuwait.

GDPR	E-Transactions Law	Cybercrime Law	General Observations
<ul style="list-style-type: none"> • monitor and enforce the application of the GDPR; • promote awareness of the risks, rules, safeguards and rights pertaining to Personal Data (especially in relation to children); • advise national and governmental institutions on the application of the GDPR; • hear claims brought by Data Subjects or their representatives, and inform Data Subjects of the outcome of such claims; • establish requirements for Impact Assessments; • encourage the creation of Codes of Conduct and review certifications; • authorise Model Clauses and BCRs; • keep records of sanctions and enforcement actions; and • fulfil "any other tasks related to protection of Personal Data". (Article 55, 57) <p>Powers</p> <p>DPSAs are empowered to oversee enforcement of the GDPR, investigate breaches of the GDPR and bring legal proceedings where necessary. (Article 58)</p>			

EGYPT



Egypt – Executive summary



Egypt does not currently have a law that regulates the protection of Personal Data. A draft law regulating the freedom of data exchange and data protection was drafted, but it has not yet been published. The cabinet in Egypt has already approved this draft law and a final version of the draft is expected in 2019.

The rules apply to Egyptian Nationals both inside and outside of the country. The law imposes various types of obligations on the controllers and processors of Personal Data and how they are entitled to handle personal information. The law's provisions ensure the rights of the citizens regarding the protection of their data. The draft law is reported to establish a committee to protect the Personal Data of the people of Egypt. It is reported that under the new proposed law, the Personal Data of people cannot be collected or disclosed by any means except with the consent of the person they concern. The appropriate person will possess the right to access and obtain their data. Unauthorised disclosures of Personal Data and other violations of the law may

lead to imprisonment for 1 year and a fine of between 100,000 to 1 million Egyptian Pounds.

The new law purports to establish a Centre for Personal Data Protection in the Information Technology Industry Development Agency (**Centre**) and a Ministerial Decision will appoint all the employees following a proposal from a competent minister. The Centre will make and formulate various policies and regulations, and will be tasked with monitoring compliance with, and enforcing the provisions of, the new law. It is expected that certain Executive Regulations pursuant to the Data Protection Law will be published in March 2019.

Aside from the proposed draft law, constitutional principles concerning individuals' rights to privacy under the Egyptian *Constitution* as well as general principles on compensation for unlawful acts under the Egyptian *Civil Code* govern the collection, use and Processing of Personal Data. There are also limited provisions contained in the *Cyber Crimes Law* (Law No 175 of 2018) and the *Penal Code* (Law No 58 of 1937).

GDPR		Cyber Crimes Law	Penal Code	General Observations
Principles of Data Processing	Lawfulness, fairness, transparency Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. (Article 5(1)(a))	Lawful basis An individual's consent must be obtained in order to process their Personal Data including disclosing any obtained by such Processing. (Article 25)	Lawful basis An individual's consent must be obtained in order to process their Personal Data including disclosing any documents obtained by such Processing. (Article 309 bis)	Status Egypt does not yet have a specific Personal Data protection law. However a draft law regulating the freedom of data exchange and data protection was drafted, but it has not yet been published. The cabinet in Egypt has already approved this draft law and a final version of the draft is expected in 2019.
	Specified purposes Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. (Article 5(1)(b))			
	Data minimisation Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. (Article 5(1)(c))			
	Accuracy Personal Data must be accurate and, where necessary, kept up to date. (Article 5(1)(d))			
	Storage limitation Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. (Article 5(1)(e))			
	Integrity and confidentiality Personal Data must be processed in a way 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. (Article 5(1)(f))			

	GDPR	Cyber Crimes Law	Penal Code	General Observations
	<p>Accountability The controller shall be responsible for and be able to demonstrate compliance with all the above principles. (Article 5(2))</p> <p>Lawful bases The legal bases under which Personal Data may be processed are:</p> <ul style="list-style-type: none"> • with the freely given, specific, informed and unambiguous consent of the Data Subject; • where necessary for the performance of a contract to which the Data Subject is party; • where necessary to comply with a legal obligation to which the controller is subject; • where necessary to protect the vital interests of the Data Subject or another person; • where 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 • where necessary for the purposes of the legitimate interests of the controller or a third party. (Article 6(1)) 			
Data Controller and Data Processor Obligations	<p>General principles The controller is responsible for compliance with the principles listed in Article 5 (as set out above).</p> <p>The controller must have regard to 'data protection by design and by default' throughout their Processing activities.</p> <p>Lawful processing The controller must carry only process Personal Data under one of the conditions</p>	<p>Data storage Telecoms service providers shall keep and store the information system log or any IT means for a period of 180 consecutive days. The data to be kept and stored shall include Personal Data that helps identify the service user. (Article 2(1))</p> <p>Confidentiality Telecoms service providers shall maintain the confidentiality of the Personal Data kept and stored, and not disclose it without</p>	<p>Consent An individual's consent must be obtained in order to process their Personal Data including disclosing any documents obtained by such Processing. (Article 309 bis)</p>	<p>The GDPR places significantly more onerous burdens on Data Controllers and Data Processors than the laws in the Egypt.</p> <p>Data Processing agreements are not governed by any laws or regulations in Egypt. No standard form or precedent data Processing agreements have been approved by the national authorities or Egyptian courts.</p>

GDPR	Cyber Crimes Law	Penal Code	General Observations
	<p>laid out in Article 6 and for special categories of Personal Data those laid out in Article 9.</p> <p>Sensitive personal data The Processing of sensitive Personal Data is prohibited, unless the:</p> <ul style="list-style-type: none"> • Data Subject has given explicit consent. (Article 9(2)(a)) • Processing is necessary in the context of employment law, or laws relating to social security and social protection. (Article 9(2)(b)) • Processing is necessary to protect vital interests of the Data Subject (or another person). (Article 9(2)(c)) • Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim. (Article 9(2)(d)) • Processing relates to Personal Data which are manifestly made public by the Data Subject. (Article 9(2)(e)) • Processing is necessary for the establishment, exercise or defence of legal claims. (Article 9(2)(f)) • Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law. (Article 9(2)(g)) • Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of 	<p>a reasoned warrant issued by a competent judicial authority. (Article 2(2))</p> <p>Security Telecoms service providers shall secure Personal Data and information in a manner that maintains its confidentiality and prevents it from being hacked or damaged. (Article 2(3))</p>	

GDPR	Cyber Crimes Law	Penal Code	General Observations
	<p>health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional. (Article 9(2)(h))</p> <ul style="list-style-type: none"> Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law. (Article 9(2)(i)) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. (Article 9(2)(j)) <p>Technical & organisational measures The controller is responsible for implementing appropriate technical and organisational measures to ensure and demonstrate that its Processing activities are compliant with the requirements of the GDPR. (Article 32)</p> <p>Data subject rights The controller must demonstrate the Data Subject's consent to Processing their Personal Data. The consent must be clearly presented and easily distinguished from other matters, in an intelligible and easily accessible form. The consent must be able to be withdrawn at any time. (Article 24)</p> <p>The controller must make reasonable efforts to verify parental consent (when the</p>		

GDPR		Cyber Crimes Law	Penal Code	General Observations
	<p>child is under 16, although in some members states may be as young as 13).</p> <p>Choosing a data processor The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of this Regulation and ensure the protection of the rights of the Data Subject.</p> <p>Processing by a processor shall be governed by a contract or other legal act. (Article 28)</p> <p>Notifications In the case of a Personal Data breach, the controller must notify the supervisory authority of the breach. This must be done without due delay and, where feasible, not later than 72 hours after having become aware of it. (Article 33)</p> <p>Record keeping Each controller must maintain a record of its Processing activities. (Article 30)</p> <p>Appoint a representative The controller must appoint an EU representative in certain situations. (Article 27)</p> <p>Appoint a DPO The controller must appoint a Data Protection Officer (DPO) in certain situations. (Article 37(1))</p>			
Data Subject Rights	<p>Transparent communication In order to ensure that Personal Data are processed fairly and lawfully, controllers must provide certain minimum information</p>	<p>Consent An individual's consent must be obtained in order to process their Personal Data</p>	<p>Consent An individual's consent must be obtained in order to process their Personal Data</p>	<p>There are only limited measures in place under Egyptian law to enable Data Subjects to vindicate their rights. There is no general protection of Data Subject</p>

GDPR	Cyber Crimes Law	Penal Code	General Observations
	<p>to Data Subjects, regarding the collection and further Processing of their Personal Data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. (Articles 5(1)(a), 12-14)</p> <p>Data subject rights Data controllers have a legal obligation to give effect to the rights of Data Subjects. (Article 12(2))</p> <p>Identifying data subjects Data controllers must not refuse to give effect to the rights of a Data Subject unless the controller cannot identify the Data Subject. The controller must use all reasonable efforts to verify the identity of Data Subjects. Where the controller has reasonable doubts as to the identity of the Data Subject, the controller may request the provision of additional information necessary to confirm the identity of the Data Subject, but is not required to do so. (Article 12(2), (6))</p> <p>Time limits A controller must, within one month of receiving a request made under those rights, provide any requested information in relation to any of the rights of Data Subjects. If the controller fails to meet this deadline, the Data Subject may complain to the relevant DPSA and may seek a judicial remedy. Where a controller receives large numbers of requests, or especially complex requests, the time limit may be extended by a maximum of two further months. (Article 12(3) - (4))</p>	<p>including disclosing any documents obtained by such Processing. (Article 25)</p>	<p>including disclosing any documents obtained by such Processing. (Article 309 bis)</p> <p>rights in line with the GDPR. Shari'a principles, the Penal Code and the Cyber Crimes Law provide merely the right not to have their personal information captured without their consent and to have the confidentiality of such information maintained.</p>

GDPR	Cyber Crimes Law	Penal Code	General Observations
<p>Basic information Data Subjects have the right to be provided with information on the identity of the controller, the reasons for Processing their Personal Data and other relevant information necessary to ensure the fair and transparent Processing of Personal Data. (Articles 13 and 14)</p> <p>Right of access Data Subjects have the right to obtain the following:</p> <ul style="list-style-type: none"> • confirmation of whether, and where, the controller is Processing their Personal Data; • information about the purposes of the Processing; • information about the categories of data being processed; • information about the categories of recipients with whom the data may be shared; • information about the period for which the data will be stored (or the criteria used to determine that period); • information about the existence of the rights to erasure, to rectification, to restriction of Processing and to object to Processing; • information about the existence of the right to complain to the DPSA; • where the data were not collected from the Data Subject, information as to the source of the data; and • information about the existence of, and an explanation of the logic involved in any automated Processing that has a significant effect on Data Subjects; and 			

GDPR	Cyber Crimes Law	Penal Code	General Observations
<ul style="list-style-type: none"> Data Subjects may request a copy of the Personal Data being processed. (Article 15) <p>Access fees Data controllers must give effect to the rights of access, rectification, erasure and the right to object, free of charge. The controller may charge a reasonable fee for "repetitive requests", "manifestly unfounded or excessive requests" or "further copies". (Articles 12(5), 15(3), (4))</p> <p>Rectification Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data Subjects have the right to rectification of inaccurate Personal Data. (Articles 5(1)(d), 16)</p> <p>Erasure Data Subjects have the right to erasure of Personal Data if:</p> <ul style="list-style-type: none"> the data are no longer needed for their original purpose (and no new lawful purpose exists); the lawful basis for the Processing is the Data Subject's consent, the Data Subject withdraws that consent, and no other lawful ground exists; the Data Subject exercises the right to object, and the controller has no overriding grounds for continuing the Processing; the data have been processed unlawfully; or erasure is necessary for compliance with EU law or the national law of the relevant Member State. (Article 17) 			

GDPR	Cyber Crimes Law	Penal Code	General Observations
<p>Restrict processing Data Subjects have the right to restrict the Processing of Personal Data (meaning that the data may only be held by the controller, and may only be used for limited purposes) if:</p> <ul style="list-style-type: none"> • the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); • the Processing is unlawful and the Data Subject requests restriction (as opposed to exercising the right to erasure); • the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or • if verification of overriding grounds is pending, in the context of an erasure request. (Article 18) <p>Portability Data Subjects have a right to:</p> <ul style="list-style-type: none"> • receive a copy of their Personal Data in a structured, commonly used, machine-readable format that supports re-use; • transfer their Personal Data from one controller to another; • store their Personal Data for further personal use on a private device; and • have their Personal Data transmitted directly between controllers without hindrance. (Article 20) <p>Object to processing Data Subjects have the right to object, on grounds relating to their particular</p>			

GDPR	Cyber Crimes Law	Penal Code	General Observations
<p>situation, to the Processing of Personal Data, where the basis for that Processing is either:</p> <ul style="list-style-type: none"> • public interest; or • legitimate interests of the controller. <p>The controller must cease such Processing unless the controller:</p> <ul style="list-style-type: none"> • demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject; or • requires the data in order to establish, exercise or defend legal rights. (Article 21) <p>Where Personal Data are processed for scientific and historical research purposes or statistical purposes, the Data Subject has the right to object, unless the Processing is necessary for the performance of a task carried out for reasons of public interest. (Articles 21(6), 83(1))</p> <p>Object to direct marketing Data Subjects have the right to object to the Processing of Personal Data for the purpose of direct marketing, including profiling. (Article 21(2) – (3))</p> <p>Duty to inform of right to object The right to object to Processing of Personal Data noted above must be communicated to the Data Subject no later than the time of the first communication with the Data Subject.</p> <p>This information should be provided clearly and separately from any other information</p>			

GDPR		Cyber Crimes Law	Penal Code	General Observations
	<p>provided to the Data Subject. (Articles 3(2)(b), 14(2)(c), 15(1)(e), 21(4))</p> <p>Automated processing Data Subjects have the right not to be subject to a decision based solely on automated Processing which significantly affect them (including profiling). Such Processing is permitted where:</p> <ul style="list-style-type: none"> • it is necessary for entering into or performing a contract with the Data Subject provided that appropriate safeguards are in place; • it is authorised by law; or • the Data Subject has explicitly consented and appropriate safeguards are in place. (Article 22) 			
Cross-Border Transfer Rules	<p>General prohibition Cross-Border Personal Data Transfers may only take place if the transfer is made to an Adequate Jurisdiction or the data exporter has implemented a lawful data transfer mechanism (or an exemption or derogation applies). (Articles 44, 45)</p> <p>Adequacy decisions Cross-border data transfers may take place if the third country receives an Adequacy Decision from the EU Commission. (Articles 44, 45)</p> <p>The EU Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the USA (subject to compliance with the terms of the US-EU Privacy Shield).</p>	<p>Consent An individual's consent must be obtained in order to transfer their Personal Data outside Egypt. (Article 25)</p>	<p>Consent to transfer An individual's consent must be obtained in order to transfer their Personal Data outside Egypt. (Article 309 bis)</p>	<p>There is no specific regulation currently dealing specifically with the transfer of Personal Data outside Egypt in line with the GDPR. Data transfer agreements are not governed by any laws or regulations in Egypt. No standard form or precedent data transfer agreements have been approved by the national authorities or Egyptian courts.</p> <p>NOTE: Under the GDPR, Cross-border data transfers may take place on the basis of standard data protection clauses approved by the EU Commission ("Model Clauses"). The current set of Model Clauses are currently being challenged as a form of appropriate data transfer mechanism; therefore their future is uncertain.</p> <p>In January 2019, the Irish Supreme Court (as part of the <i>Schrems v Facebook</i></p>

GDPR	Cyber Crimes Law	Penal Code	General Observations
<p>Public Authorities Cross-border data transfers between public authorities may take place under agreements between public authorities, which do not require any specific authorisation from a DPSA. (Articles 46(2)(a), 46(3)(b))</p> <p>Binding Corporate Rules Cross-Border Data Transfer within a corporate group may take place on the basis of Binding Corporate Rules ("BCRs"). BCRs require approval from DPSAs, but approved, individual transfers made under the BCRs do not require further approval. (Articles 4(20) 46(2)(b), 47)</p> <p>Model clauses Cross-border data transfers may take place on the basis of the Model Clauses entered into between the data exporter and data recipient. Existing Model Clauses implemented under the 1995 Directive remain valid until amended, replaced or repealed under the GDPR. (Articles 28(6)-(8), 46(2)(c), 57(1)(j), (r), 93(2))</p> <p>Other mechanisms Cross-border data transfers may take place on the basis, <i>inter alia</i>, of:</p> <ul style="list-style-type: none"> • standard data protection clauses adopted by one or more DPSAs under the GDPR. (Articles 46(2)(d), 64(1)(d), 57(1)(j), (r), 93(2)) • an approved code of conduct, together with binding and enforceable commitments to provide appropriate safeguards. (Articles 40, 41, 46(2)(e)) • certifications together with binding and enforceable commitments of the data 			<p>litigation) heard an appeal by Facebook over a decision of the Irish High Court to refer a number of questions to the Court of Justice of the EU ("CJEU") regarding the validity of this data transfer mechanism. The Supreme Court will publish its decision in due course. If Facebook is unsuccessful in its appeal, the CJEU will rule on these questions, which may result in a declaration that the Model Clauses are no longer valid as a transfer mechanism.</p>

GDPR	Cyber Crimes Law	Penal Code	General Observations
	<p>importer to apply the certification to the transferred data. (Articles 42, 43, 46(2)(f))</p> <ul style="list-style-type: none"> ad hoc clauses conforming to the GDPR and approved by the relevant DPSA. (Articles 46(3)(a), (4), 63)) administrative arrangements between public authorities (e.g., MOUs) subject DPSA approval. (Articles 46(3)(b), (4), 63) <p>Derogations Cross-border data transfers may be made on the basis, <i>inter alia</i>, that:</p> <ul style="list-style-type: none"> the Data Subject explicitly consents having been informed of the possible risks of such transfer. (Article 49(1)(a), (3)) the performance of a contract between the Data Subject and the controller. (Article 49(1)(b), (3)) it is necessary for the purposes of performing or concluding a contract in the interests of the Data Subject. (Article 49(1)(c), (3)) the transfer is necessary for important reasons of public interest. (Article 49(1)(d), (4)) it is necessary for the purposes of legal proceedings, or obtaining legal advice. (Article 49(1)(e)) the transfer is necessary in order to protect the vital interests of the Data Subject, where the Data Subject is incapable of giving consent. (Article 49(1)(f)) the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by those of the individual subject to informing the relevant DPSA and the Data Subjects. (Article 49(1), (3), (6)) 		

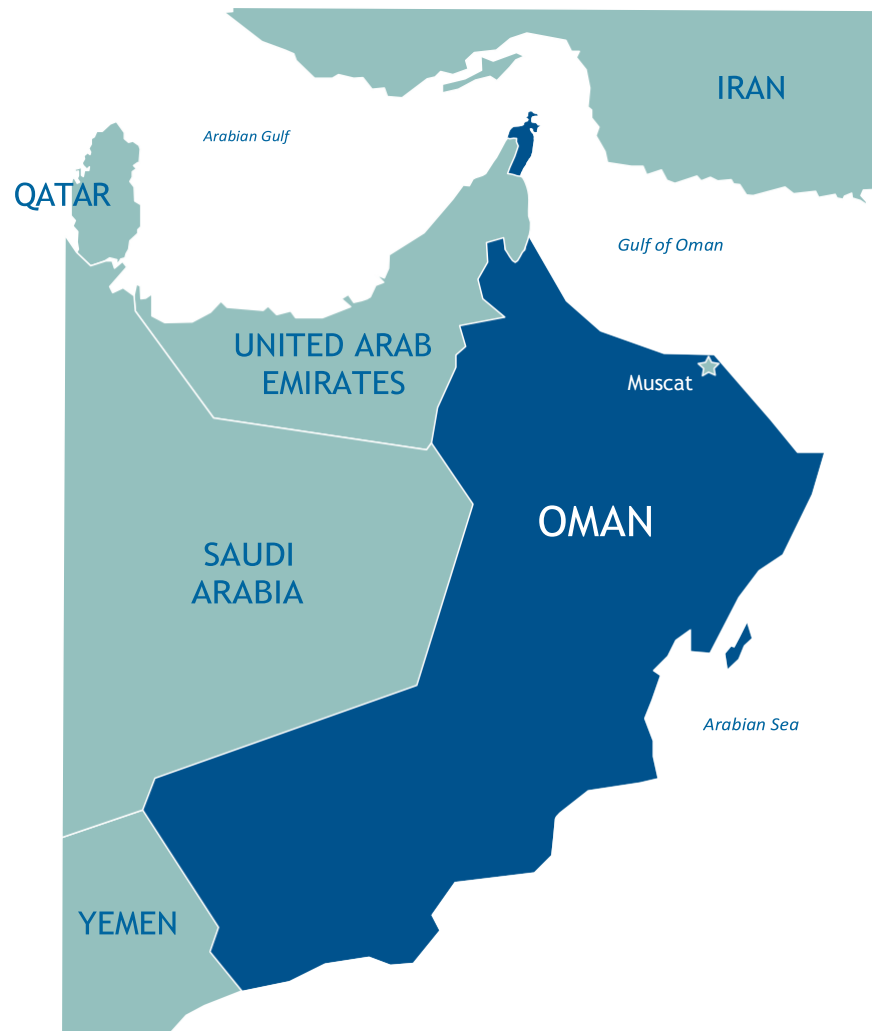
GDPR		Cyber Crimes Law	Penal Code	General Observations
Personal Data Security	<p>Security Data controllers must implement appropriate technical and organisational security measures to protect Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.</p> <p>Depending on the nature of the Processing, these measures may include:</p> <ul style="list-style-type: none"> • encryption of the Personal Data; • on-going reviews of security measures; • redundancy and back-up facilities; and • regular security testing. (Article 32) 	<p>Security Telecoms service providers shall secure Personal Data and information in a manner that maintains its confidentiality and prevents it from being hacked or damaged. (Article 2(3))</p>	No specific relevant provisions exist.	There are no specific provisions relating to Personal Data security outside the requirement to maintain the confidentiality of such data and prevent it from being hacked under the Cyber Crimes Law.
Administrative Fines and Regulatory Sanctions	<p>Judicial remedies Data Subjects have the right to an effective judicial remedy against:</p> <ul style="list-style-type: none"> • decisions of a DPSA concerning them; • any failure by a DPSA to deal with, or respond to, a complaint within three months; and • any unlawful Processing of their Personal Data by a controller or processor. (Article 78-79) <p>Compensation & liability A Data Subject who has suffered harm as a result of the unlawful Processing of his or her Personal Data has the right to receive compensation from the controller or processor for the harm suffered:</p> <ul style="list-style-type: none"> • Any controller involved in the Processing is liable for the harm caused. • A processor is liable for the harm caused by any of its (or its sub-processor's) Processing activities that 	<p>Disclosure, communications Anyone who sends large amounts of e-mails to a particular person without his consent, provides his Personal Data to an electronic system or a website for the promotion of goods or services without his consent, or publishes through the information network or any IT means information, news, images or the like, that violates the privacy of any person without his consent, whether the published information is true or not, shall be subject to:</p> <ul style="list-style-type: none"> • imprisonment for a period of not less than 6 months; and/or • a fine between 50,000 - 100,000 Egyptian Pounds. (Article 25) <p>Public morals Anyone who deliberately uses an information program or an information technology in Processing Personal Data to associate it with content that is contrary to public morals or to show them in a way that</p>	<p>Eavesdropping, recording Anyone who is found to be encroaching on the private life of another, without consent, by eavesdropping, recording, transmitting talks taking place in private places or via telephones, in addition to taking or transmission of photos of a person in a private place shall be subject to imprisonment for a maximum of 1 year. (Article 309 bis)</p> <p>If the results of such actions are the disclosure, use and divulgence of the documents obtained by the methods provided above, the person shall be subject to imprisonment for a maximum of 5 years. (Article 309 bis A)</p>	<p>The absence of a national data protection supervisory authority means that there is no effective supervision and/or enforcement of Data Subject rights or data protection principles in Egypt.</p> <p>Cyber crimes are punished by the National Telecommunication Regulatory Authority and penalties are imposed for identity theft, electronic marketing without consent, electronic piracy, email theft and other unlawful activities.</p>

GDPR	Cyber Crimes Law	Penal Code	General Observations
<p>are not in compliance with its obligations under the GDPR, or are in breach of the controller's instructions.</p> <ul style="list-style-type: none"> To ensure effective compensation, each controller or processor will be held liable for the entirety of the harm caused, if they are involved in the same Processing and responsible for that harm. (Article 82(1)-(2), (4)) <p>Joint-controller liability Data Subjects are entitled to enforce their rights against any of the joint controllers. Each joint controller is liable for the entirety of the damage, although national law may apportion liability between them. If one joint controller has paid full compensation, it may then bring proceedings against the other joint controllers to recover their portions of the damages. (Article 26(3), 82(3)-(5))</p> <p>Exemptions from liability A controller or processor is exempt from liability if it proves that it is not responsible for the event giving rise to the harm. There is no mention of force majeure events. (Article 82(3))</p> <p>Administrative fines The maximum fine that can be imposed for serious infringements of the GDPR is the greater of €20 million or 4% of an undertaking's worldwide turnover for the preceding financial year. (Article 83(5) – (6))</p> <p>Fine criteria When deciding whether to impose a fine and deciding on the amount, DPSAs are required to give due regard to a range of issues, including:</p>	<p>would prejudice their position or honour, shall be subject to:</p> <ul style="list-style-type: none"> imprisonment for a period between 2 – 5 years; and/or a fine between 100,000 – 300,000 Egyptian Pounds. (Article 26) 		

GDPR		Cyber Crimes Law	Penal Code	General Observations
	<ul style="list-style-type: none"> the nature, gravity and duration of the infringement; the number of Data Subjects affected and the level of harm suffered by them; the intentional or negligent character of the infringement; any action taken by the controller or processor to mitigate the harm; any relevant previous infringements by the controller or processor; the degree of co-operation with the relevant DPSA; whether the infringement was self-reported by the controller or processor; and any other aggravating or mitigating factors. (Article 82(3)) 			
Role and Powers of any relevant Data Protection Supervisory Authority	<p>Independence DPSAs must act independently and operate free from all outside influences, including government control. (Article 52)</p> <p>Tasks The tasks of DPSAs include obligations to:</p> <ul style="list-style-type: none"> monitor and enforce the application of the GDPR; promote awareness of the risks, rules, safeguards and rights pertaining to Personal Data (especially in relation to children); advise national and governmental institutions on the application of the GDPR; hear claims brought by Data Subjects or their representatives, and inform Data Subjects of the outcome of such claims; 	The law is enforced by the National Telecommunication Regulatory Authority.	The law is enforced by the Minister of Justice.	The absence of a national data protection supervisory authority means that there is no effective supervision and/or enforcement of Data Subject rights or data protection principles in Egypt.

GDPR	Cyber Crimes Law	Penal Code	General Observations
<ul style="list-style-type: none"> • establish requirements for Impact Assessments; • encourage the creation of Codes of Conduct and review certifications; • authorise Model Clauses and BCRs; • keep records of sanctions and enforcement actions; and • fulfil "any other tasks related to protection of Personal Data". (Article 55, 57) <p>Powers DPSAs are empowered to oversee enforcement of the GDPR, investigate breaches of the GDPR and bring legal proceedings where necessary. (Article 58)</p>			

OMAN



Oman – Executive summary



The Sultanate of Oman does not currently have a specific privacy or data protection law. Whilst Oman's *Constitution* (Royal Decree No 101 of 96) recognises individuals' rights to confidentiality in all forms of communication, it does not recognise the right to privacy as a fundamental right beyond this.

The Oman Information Technology Authority (**ITA**) announced in 2017 that it was developing a data protection law, however the law remains a draft without a clear indication of when it will be promulgated. It was reported that if approved and signed into law, the law will grant powerful rights to individuals in Oman, enabling them to:

- object to the Processing of their Personal Data;
- demand access to any Personal Data about them held by any organisation in Oman;
- demand that any mistakes in this data are corrected; and
- demand that this data is completely erased if they wish.

The ITA went as far as to have public consultation sessions to discuss this draft law and seek feedback from members of the public on its contents but no further developments have occurred.

A limited number of other laws in Oman relate to the use of personal information, however these are not the equivalent of bespoke data protection laws such as the GDPR. The *Electronic Transactions Law* (Royal Decree No 69 of 2008), which is based largely on the UN Model Laws relating to e-commerce and electronic signatures, contains limited provisions relating to the Processing of Personal Data as well as requirements relating to the obtaining, retention and dissemination of Personal Data. Whilst this law is perhaps better developed around the principles of Personal Data protection, it only applies to transactions performed between parties who have agreed to perform their transactions electronically. Therefore its narrow data protection provisions do not apply to those who collect personal information outside the scope of this law.

The *Cyber Crime Law* (Royal Decree No 12 of 2011) also contains limited provisions with respect to Personal Data protection including making it an offence to violate the privacy of individuals using technology. It does not however impose any obligations on those who collect private Personal Data.

	GDPR	Electronic Transactions Law	Cyber Crime Law	General Observations
Principles of Data Processing	<p>Lawfulness, fairness, transparency Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. (Article 5(1)(a))</p> <p>Specified purposes Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. (Article 5(1)(b))</p> <p>Data minimisation Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. (Article 5(1)(c))</p> <p>Accuracy Personal Data must be accurate and, where necessary, kept up to date. (Article 5(1)(d))</p> <p>Storage limitation Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. (Article 5(1)(e))</p> <p>Integrity and confidentiality Personal Data must be processed in a way 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. (Article 5(1)(f))</p>	<p>Lawful processing Any person controlling Personal Data is forbidden to process these data if the Processing will cause damage to persons from whom such data is collected or will prejudice their rights and freedoms. (Article 48)</p> <p>Specified purposes Government bodies and authentication service providers may collect Personal Data directly from the Data Subject or from others after his explicit approval, only for the purposes of:</p> <ul style="list-style-type: none"> • issuing a certificate or keeping it or facilitating such issuing or keeping; • if these data are necessary to prevent or discover a crime on official request from the investigation authorities; • if these data are required or authorised by any law or by a court decision; • if these data are necessary for the estimation or collection of any taxes or fees; or • if the Processing is necessary for the protection of the Data Subject. (Article 43) <p>It is not permitted to collect or process or use such data for any other purpose without the explicit consent of the Data Subject. (Article 43)</p> <p>Confidentiality The authentication service provider shall follow the appropriate procedure to ensure confidentiality of the Personal Data in his possession in the course of his business and he shall not disclose or transfer,</p>	<p>Lawful basis An individual's consent must be obtained in order to process their Personal Data including disclosing any documents obtained by such Processing.</p>	<p>Status A specific data protection law has been expected for some time, but as of yet there is still no statutory law governing data protection in place. The Electronic Transactions Law imposes certain obligations in respect of the handling, Processing and transfer of Personal Data but only applies to electronic transactions (albeit widely defined).</p> <p>Looking forward There were reports in 2017 that ITA was working on a first draft of a data protection law for Oman, and that public consultation sessions went ahead to discuss this draft law and seek feedback from members of the public on its contents. However, there is no recent information on this law and thus no clear indication of when such law will be promulgated.</p> <p>Very limited information is available about the draft law, but it has been suggested that it will include Data Subject rights in line with those included in the GDPR.</p> <p>It is speculated that the draft law includes the right of Data Subjects to object to the Processing of their Personal Data, demand access to any Personal Data held about them by any organisation in Oman, demand that any mistakes in this data are rectified, and demand that their data be erased if they wish.</p>

	GDPR	Electronic Transactions Law	Cyber Crime Law	General Observations
	<p>Accountability The controller shall be responsible for and be able to demonstrate compliance with all the above principles. (Article 5(2))</p> <p>Lawful bases The legal bases under which Personal Data may be processed are:</p> <ul style="list-style-type: none"> • with the freely given, specific, informed and unambiguous consent of the Data Subject; • where necessary for the performance of a contract to which the Data Subject is party; • where necessary to comply with a legal obligation to which the controller is subject; • where necessary to protect the vital interests of the Data Subject or another person; • where 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 • where necessary for the purposes of the legitimate interests of the controller or a third party. (Article 6(1)) 	<p>declare or publicise these data for any purpose. (Article 44)</p> <p>Transparency Any person who controls Personal Data by virtue of his job in electronic transactions shall notify the Data Subject before Processing such data. This notification shall be via a 'designated notice' and shall include:</p> <ul style="list-style-type: none"> • an identification of the person responsible for Processing the data; • the nature of the data, and the purpose, methods; and • locations of Processing and security measures. (Article 45) 		
<p>Data Controller and Data Processor Obligations</p>	<p>General principles The controller is responsible for compliance with the principles listed in Article 5 (as set out above).</p> <p>The controller must have regard to 'data protection by design and by default' throughout their Processing activities.</p> <p>Lawful processing The controller must carry only process Personal Data under one of the conditions</p>	<p>There is no concept of 'data controller' in this law. The most similar concept is the mention to 'any person controlling Personal Data'.</p> <p>Lawful processing Any person controlling Personal Data cannot process these data if the Processing will cause damage to the Data Subject or will prejudice their rights and freedoms. (Article 48)</p>	<p>Lawful basis An individual's consent must be obtained in order to process their Personal Data including disclosing any documents obtained by such Processing.</p>	<p>Omani laws recognise that Personal Data form part of the fundamental rights and freedoms of individuals.</p> <p>The GDPR places significantly more onerous burdens on Data Controllers and Data Processors than any law in Oman.</p> <p>Data Processing agreements are not governed by any laws or regulations in Oman. No standard form or precedent data Processing agreements have been</p>

GDPR	Electronic Transactions Law	Cyber Crime Law	General Observations
<p>laid out in Article 6 and for special categories of Personal Data those laid out in Article 9.</p> <p>Sensitive personal data The Processing of sensitive Personal Data is prohibited, unless the:</p> <ul style="list-style-type: none"> • Data Subject has given explicit consent. (Article 9(2)(a)) • Processing is necessary in the context of employment law, or laws relating to social security and social protection. (Article 9(2)(b)) • Processing is necessary to protect vital interests of the Data Subject (or another person). (Article 9(2)(c)) • Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim. (Article 9(2)(d)) • Processing relates to Personal Data which are manifestly made public by the Data Subject. (Article 9(2)(e)) • Processing is necessary for the establishment, exercise or defence of legal claims. (Article 9(2)(f)) • Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law. (Article 9(2)(g)) • Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of 			<p>approved by the national authorities or Oman courts.</p>

GDPR	Electronic Transactions Law	Cyber Crime Law	General Observations
	<p>health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional. (Article 9(2)(h))</p> <ul style="list-style-type: none"> Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law. (Article 9(2)(i)) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. (Article 9(2)(j)) <p>Technical & organisational measures The controller is responsible for implementing appropriate technical and organisational measures to ensure and demonstrate that its Processing activities are compliant with the requirements of the GDPR. (Article 32)</p> <p>Data subject rights The controller must demonstrate the Data Subject's consent to Processing their Personal Data. The consent must be clearly presented and easily distinguished from other matters, in an intelligible and easily accessible form. The consent must be able to be withdrawn at any time. (Article 24)</p> <p>The controller must make reasonable efforts to verify parental consent (when the</p>		

GDPR	Electronic Transactions Law	Cyber Crime Law	General Observations
<p>child is under 16, although in some members states may be as young as 13).</p> <p>Choosing a data processor The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of this Regulation and ensure the protection of the rights of the Data Subject.</p> <p>Processing by a processor shall be governed by a contract or other legal act. (Article 28)</p> <p>Notifications In the case of a Personal Data breach, the controller must notify the supervisory authority of the breach. This must be done without due delay and, where feasible, not later than 72 hours after having become aware of it. (Article 33)</p> <p>Record keeping Each controller must maintain a record of its Processing activities. (Article 30)</p> <p>Appoint a representative The controller must appoint an EU representative in certain situations. (Article 27)</p> <p>Appoint a DPO The controller must appoint a Data Protection Officer (DPO) in certain situations. (Article 37(1))</p>			
<p>Data Subject Rights</p>	<p>Transparent communication In order to ensure that Personal Data are processed fairly and lawfully, controllers must provide certain minimum information</p>	<p>Right of access The authentication service provider shall, upon the request of the person from whom data is collected, enable that person to</p>	<p>No specific relevant provisions exist.</p> <p>There are only limited measures in place under Oman law to enable Data Subjects to vindicate their rights. There is no general protection of Data Subject rights in line with</p>

GDPR	Electronic Transactions Law	Cyber Crime Law	General Observations
<p>to Data Subjects, regarding the collection and further Processing of their Personal Data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. (Articles 5(1)(a), 12-14)</p> <p>Data subject rights Data controllers have a legal obligation to give effect to the rights of Data Subjects. (Article 12(2))</p> <p>Identifying data subjects Data controllers must not refuse to give effect to the rights of a Data Subject unless the controller cannot identify the Data Subject. The controller must use all reasonable efforts to verify the identity of Data Subjects. Where the controller has reasonable doubts as to the identity of the Data Subject, the controller may request the provision of additional information necessary to confirm the identity of the Data Subject, but is not required to do so. (Article 12(2), (6))</p> <p>Time limits A controller must, within one month of receiving a request made under those rights, provide any requested information in relation to any of the rights of Data Subjects. If the controller fails to meet this deadline, the Data Subject may complain to the relevant DPSA and may seek a judicial remedy. Where a controller receives large numbers of requests, or especially complex requests, the time limit may be extended by a maximum of two further months. (Article 12(3) - (4))</p>	<p>have access to or update those Personal Data.</p> <p>Such right shall include the right of accessing all Personal Databases related to the person from whom it is collected, and shall make available to him all the appropriate technical means for this purpose. (Article 46)</p> <p>Right of rectification Individuals have the right to update their Personal Data. (Article 46)</p> <p>Right to refuse Individuals have the right to refuse to accept electronic documents that have been sent to them. (Article 47)</p>		<p>the GDPR. Shari'a principles, the Constitution and the Electronic Transactions Law provide the right not to have their personal information captured without their consent and to have the confidentiality of such information maintained.</p>

GDPR	Electronic Transactions Law	Cyber Crime Law	General Observations
<p>Basic information Data Subjects have the right to be provided with information on the identity of the controller, the reasons for Processing their Personal Data and other relevant information necessary to ensure the fair and transparent Processing of Personal Data. (Articles 13 and 14)</p> <p>Right of access Data Subjects have the right to obtain the following:</p> <ul style="list-style-type: none"> • confirmation of whether, and where, the controller is Processing their Personal Data; • information about the purposes of the Processing; • information about the categories of data being processed; • information about the categories of recipients with whom the data may be shared; • information about the period for which the data will be stored (or the criteria used to determine that period); • information about the existence of the rights to erasure, to rectification, to restriction of Processing and to object to Processing; • information about the existence of the right to complain to the DPSA; • where the data were not collected from the Data Subject, information as to the source of the data; and • information about the existence of, and an explanation of the logic involved in any automated Processing that has a significant effect on Data Subjects; and 			

GDPR	Electronic Transactions Law	Cyber Crime Law	General Observations
<ul style="list-style-type: none"> Data Subjects may request a copy of the Personal Data being processed. (Article 15) <p>Access fees Data controllers must give effect to the rights of access, rectification, erasure and the right to object, free of charge. The controller may charge a reasonable fee for "repetitive requests", "manifestly unfounded or excessive requests" or "further copies". (Articles 12(5), 15(3), (4))</p> <p>Rectification Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data Subjects have the right to rectification of inaccurate Personal Data. (Articles 5(1)(d), 16)</p> <p>Erasure Data Subjects have the right to erasure of Personal Data if:</p> <ul style="list-style-type: none"> the data are no longer needed for their original purpose (and no new lawful purpose exists); the lawful basis for the Processing is the Data Subject's consent, the Data Subject withdraws that consent, and no other lawful ground exists; the Data Subject exercises the right to object, and the controller has no overriding grounds for continuing the Processing; the data have been processed unlawfully; or erasure is necessary for compliance with EU law or the national law of the relevant Member State. (Article 17) 			

GDPR	Electronic Transactions Law	Cyber Crime Law	General Observations
<p>Restrict processing Data Subjects have the right to restrict the Processing of Personal Data (meaning that the data may only be held by the controller, and may only be used for limited purposes) if:</p> <ul style="list-style-type: none"> • the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); • the Processing is unlawful and the Data Subject requests restriction (as opposed to exercising the right to erasure); • the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or • if verification of overriding grounds is pending, in the context of an erasure request. (Article 18) <p>Portability Data Subjects have a right to:</p> <ul style="list-style-type: none"> • receive a copy of their Personal Data in a structured, commonly used, machine-readable format that supports re-use; • transfer their Personal Data from one controller to another; • store their Personal Data for further personal use on a private device; and • have their Personal Data transmitted directly between controllers without hindrance. (Article 20) 			

GDPR	Electronic Transactions Law	Cyber Crime Law	General Observations
<p>Object to processing Data Subjects have the right to object, on grounds relating to their particular situation, to the Processing of Personal Data, where the basis for that Processing is either:</p> <ul style="list-style-type: none"> • public interest; or • legitimate interests of the controller. <p>The controller must cease such Processing unless the controller:</p> <ul style="list-style-type: none"> • demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject; or • requires the data in order to establish, exercise or defend legal rights. (Article 21) <p>Where Personal Data are processed for scientific and historical research purposes or statistical purposes, the Data Subject has the right to object, unless the Processing is necessary for the performance of a task carried out for reasons of public interest. (Articles 21(6), 83(1))</p> <p>Object to direct marketing Data Subjects have the right to object to the Processing of Personal Data for the purpose of direct marketing, including profiling. (Article 21(2) – (3))</p> <p>Duty to inform of right to object The right to object to Processing of Personal Data noted above must be communicated to the Data Subject no later than the time of the first communication with the Data Subject.</p>			

GDPR	Electronic Transactions Law	Cyber Crime Law	General Observations
	<p>This information should be provided clearly and separately from any other information provided to the Data Subject. (Articles 3(2)(b), 14(2)(c), 15(1)(e), 21(4))</p> <p>Automated processing Data Subjects have the right not to be subject to a decision based solely on automated Processing which significantly affect them (including profiling). Such Processing is permitted where:</p> <ul style="list-style-type: none"> • it is necessary for entering into or performing a contract with the Data Subject provided that appropriate safeguards are in place; • it is authorised by law; or • the Data Subject has explicitly consented and appropriate safeguards are in place. (Article 22) 		
<p>Cross-Border Transfer Rules</p>	<p>General prohibition Cross-Border Personal Data Transfers may only take place if the transfer is made to an Adequate Jurisdiction or the data exporter has implemented a lawful data transfer mechanism (or an exemption or derogation applies). (Articles 44, 45)</p> <p>Adequacy decisions Cross-border data transfers may take place if the third country receives an Adequacy Decision from the EU Commission. (Articles 44, 45)</p> <p>The EU Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the</p>	<p>General prohibition The authentication provider is forbidden to transfer Personal Data in his possession for any purpose unless an exception listed in Article 43 applies.</p> <p>Security When the Personal Data are to be transferred outside Oman, regard shall be had to the security of such information, in particular:</p> <ul style="list-style-type: none"> • the nature of Personal Data; • the source of information and data; • the purpose for which the data are to be processed and duration of process; • the country of destination where the data were transferred, its international obligation, and the law applicable; 	<p>No specific relevant provisions exist.</p> <p>There is no specific regulation currently dealing specifically with the transfer of Personal Data outside Oman in line with the GDPR. Data transfer agreements are not governed by any laws or regulations in Oman. No standard form or precedent data transfer agreements have been approved by the national authorities or Oman courts.</p> <p>NOTE: Under the GDPR, Cross-border data transfers may take place on the basis of standard data protection clauses approved by the EU Commission ("Model Clauses"). The current set of Model Clauses are currently being challenged as a form of appropriate data transfer mechanism; therefore their future is uncertain.</p>

GDPR	Electronic Transactions Law	Cyber Crime Law	General Observations
<p>USA (subject to compliance with the terms of the US-EU Privacy Shield).</p> <p>Public authorities Cross-border data transfers between public authorities may take place under agreements between public authorities, which do not require any specific authorisation from a DPSA. (Articles 46(2)(a), 46(3)(b))</p> <p>Binding Corporate Rules Cross-Border Data Transfer within a corporate group may take place on the basis of Binding Corporate Rules ("BCRs"). BCRs require approval from DPSAs, but approved, individual transfers made under the BCRs do not require further approval. (Articles 4(20) 46(2)(b), 47)</p> <p>Model clauses Cross-border data transfers may take place on the basis of the Model Clauses entered into between the data exporter and data recipient. Existing Model Clauses implemented under the 1995 Directive remain valid until amended, replaced or repealed under the GDPR. (Articles 28(6)-(8), 46(2)(c), 57(1)(j), (r), 93(2))</p> <p>Other mechanisms Cross-border data transfers may take place on the basis, <i>inter alia</i>, of:</p> <ul style="list-style-type: none"> standard data protection clauses adopted by one or more DPSAs under the GDPR. (Articles 46(2)(d), 64(1)(d), 57(1)(j), (r), 93(2)) an approved code of conduct, together with binding and enforceable 	<ul style="list-style-type: none"> any related rules applied in that country; and the security measures taken to secure that data in that country. (Article 49) 		<p>In January 2019, the Irish Supreme Court (as part of the <i>Schrems v Facebook</i> litigation) heard an appeal by Facebook over a decision of the Irish High Court to refer a number of questions to the Court of Justice of the EU ("CJEU") regarding the validity of this data transfer mechanism. The Supreme Court will publish its decision in due course. If Facebook is unsuccessful in its appeal, the CJEU will rule on these questions, which may result in a declaration that the Model Clauses are no longer valid as a transfer mechanism.</p> <p>NOTE: Under <i>Resolution No 113 of 2009 issuing Regulations on Protection of the Confidentiality and Privacy of Beneficiary Data</i> issued pursuant to <i>Royal Decree No 30 of 2002</i> (the Telecommunications Law), following the written approval of a customer, a telecom service provider (TSP) is permitted to share customer Personal Data with any of its subsidiaries or with other companies. No indication is given of whether this would include third parties outside Oman. Under such circumstances, the TSP is obliged to guarantee not to use customer data for any purpose other than the specified purposes and within the permissible limits.</p>

GDPR	Electronic Transactions Law	Cyber Crime Law	General Observations
	<p>commitments to provide appropriate safeguards. (Articles 40, 41, 46(2)(e))</p> <ul style="list-style-type: none"> • certifications together with binding and enforceable commitments of the data importer to apply the certification to the transferred data. (Articles 42, 43, 46(2)(f)) • ad hoc clauses conforming to the GDPR and approved by the relevant DPSA. (Articles 46(3)(a), (4), 63)) • administrative arrangements between public authorities (e.g., MOUs) subject DPSA approval. (Articles 46(3)(b), (4), 63) <p>Derogations Cross-border data transfers may be made on the basis, <i>inter alia</i>, that:</p> <ul style="list-style-type: none"> • the Data Subject explicitly consents having been informed of the possible risks of such transfer. (Article 49(1)(a), (3)) • the performance of a contract between the Data Subject and the controller. (Article 49(1)(b), (3)) • it is necessary for the purposes of performing or concluding a contract in the interests of the Data Subject. (Article 49(1)(c), (3)) • the transfer is necessary for important reasons of public interest. (Article 49(1)(d), (4)) • it is necessary for the purposes of legal proceedings, or obtaining legal advice. (Article 49(1)(e)) • the transfer is necessary in order to protect the vital interests of the Data Subject, where the Data Subject is incapable of giving consent. (Article 49(1)(f)) • the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller 		

GDPR		Electronic Transactions Law	Cyber Crime Law	General Observations
	which are not overridden by those of the individual subject to informing the relevant DPSC and the Data Subjects. (Article 49(1), (3), (6))			
Personal Data Security	<p>Security Data controllers must implement appropriate technical and organisational security measures to protect Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.</p> <p>Depending on the nature of the Processing, these measures may include:</p> <ul style="list-style-type: none"> • encryption of the Personal Data; • on-going reviews of security measures; • redundancy and back-up facilities; and • regular security testing. (Article 32) 	<p>Security When the Personal Data are supposed to be transferred outside Oman, regard shall be had to the security of such information, in particular:</p> <ul style="list-style-type: none"> • the nature of Personal Data; • the source of information and data; • the purpose for which the data are to be processed and duration of Processing; • the country or destination where the data were transferred, its international obligation, and the law applicable; • any related rules applied in that country; and • the security measures taken to secure the data in that country. (Article 49) 	No specific relevant provisions exist.	There are no specific provisions relating to Personal Data security outside the requirement to have regard to the security of such information under the Electronic Transactions Law. No guidance is provided as to what security measures should be deployed.
Administrative Fines and Regulatory Sanctions	<p>Judicial remedies Data Subjects have the right to an effective judicial remedy against:</p> <ul style="list-style-type: none"> • decisions of a DPSC concerning them; • any failure by a DPSC to deal with, or respond to, a complaint within three months; and • any unlawful Processing of their Personal Data by a controller or processor. (Article 78-79) <p>Compensation & liability A Data Subject who has suffered harm as a result of the unlawful Processing of his or her Personal Data has the right to receive compensation from the controller or processor for the harm suffered:</p>	<p>Penalties Stealing information, using the information contained in the computers for an illegal purpose, or intentionally, without authorisation, disclosing confidential data, carry the following penalties:</p> <ul style="list-style-type: none"> • imprisonment for a period not exceeding 2 years; and/or • a fine not exceeding 5,000 Omani Riyals. (Article 52) <p>Confiscation In addition to any punishment, the court may also confiscate tools used in the commission of the crime. (Article 54)</p>	<p>Deletion of personal data Anyone who intentionally and illegally accesses an electronic site, information system, information technology tools or a part of it, or who exceeds his authorised access or continues his existence therein after being aware of his access, and such actions result in deletion, change, amendment, disfigurement, mischief, copying, destruction or re-dissemination of Personal Data saved in the informational system or causes damage to users or beneficiaries, shall be subject to:</p> <ul style="list-style-type: none"> • imprisonment for a period between 1 and 3 years; and/or • a fine between 1,000 – 3,000 Omani Riyals. (Article 3) 	<p>The absence of a national data protection supervisory authority means that there is no effective supervision and/or enforcement of Data Subject rights or data protection principles in Oman.</p> <p>Cybercrimes are punished and penalties are imposed for stealing information, identity theft, deleting data without consent, electronic marketing without consent, electronic piracy, failing to keep data confidential, medical data theft and other unlawful activities.</p>

GDPR	Electronic Transactions Law	Cyber Crime Law	General Observations
<ul style="list-style-type: none"> Any controller involved in the Processing is liable for the harm caused. A processor is liable for the harm caused by any of its (or its sub-processor's) Processing activities that are not in compliance with its obligations under the GDPR, or are in breach of the controller's instructions. To ensure effective compensation, each controller or processor will be held liable for the entirety of the harm caused, if they are involved in the same Processing and responsible for that harm. (Article 82(1)-(2), (4)) <p>Joint-controller liability Data Subjects are entitled to enforce their rights against any of the joint controllers. Each joint controller is liable for the entirety of the damage, although national law may apportion liability between them. If one joint controller has paid full compensation, it may then bring proceedings against the other joint controllers to recover their portions of the damages. (Article 26(3), 82(3)-(5))</p> <p>Exemptions from liability A controller or processor is exempt from liability if it proves that it is not responsible for the event giving rise to the harm. There is no mention of force majeure events. (Article 82(3))</p> <p>Administrative fines The maximum fine that can be imposed for serious infringements of the GDPR is the greater of €20 million or 4% of an undertaking's worldwide turnover for the preceding financial year. (Article 83(5) – (6))</p>		<p>Medical data Any person who changes, alters, amends or intentionally or illegally destroys by using information technology tools, data or electronic information related to a medical report, diagnosis, treatment or medical care saved in an informational system or information technology tool, shall be subject to:</p> <ul style="list-style-type: none"> imprisonment for a period between 1 month and 3 years; and/or a fine between 1,000 – 10,000 Omani Riyals. (Article 5) <p>Confidential data Any person who intentionally and illegally accesses an electronic site or informational system with the intent to obtain data or governmental electronic information of a confidential nature with the result of deleting, changing, amending, disfiguring, destroying, copying, damaging or disseminating of data or electronic information shall be subject to:</p> <ul style="list-style-type: none"> imprisonment for a period between 3 and 10 years; and/or a fine between 3,000 – 10,000 Omani Riyals. (Article 5) 	

GDPR		Electronic Transactions Law	Cyber Crime Law	General Observations
	<p>Fine criteria When deciding whether to impose a fine and deciding on the amount, DPSAs are required to give due regard to a range of issues, including:</p> <ul style="list-style-type: none"> the nature, gravity and duration of the infringement; the number of Data Subjects affected and the level of harm suffered by them; the intentional or negligent character of the infringement; any action taken by the controller or processor to mitigate the harm; any relevant previous infringements by the controller or processor; the degree of co-operation with the relevant DPSA; whether the infringement was self-reported by the controller or processor; and any other aggravating or mitigating factors. (Article 82(3)) 			
Role and Powers of any relevant Data Protection Supervisory Authority	<p>Independence DPSAs must act independently and operate free from all outside influences, including government control. (Article 52)</p> <p>Tasks The tasks of DPSAs include obligations to:</p> <ul style="list-style-type: none"> monitor and enforce the application of the GDPR; promote awareness of the risks, rules, safeguards and rights pertaining to Personal Data (especially in relation to children); 	No specific relevant provisions exist.	No specific relevant provisions exist.	The absence of a national data protection supervisory authority means that there is no effective supervision and/or enforcement of Data Subject rights or data protection principles in Oman.

GDPR	Electronic Transactions Law	Cyber Crime Law	General Observations
<ul style="list-style-type: none"> • advise national and governmental institutions on the application of the GDPR; • hear claims brought by Data Subjects or their representatives, and inform Data Subjects of the outcome of such claims; • establish requirements for Impact Assessments; • encourage the creation of Codes of Conduct and review certifications; • authorise Model Clauses and BCRs; • keep records of sanctions and enforcement actions; and • fulfil "any other tasks related to protection of Personal Data". (Article 55, 57) <p>Powers DPSAs are empowered to oversee enforcement of the GDPR, investigate breaches of the GDPR and bring legal proceedings where necessary. (Article 58)</p>			

BAHRAIN



Bahrain – Executive summary



This jurisdictional overview is based on an unofficial English translation of the Personal Data Protection Law (Law No 30 of 2018). An official English translation is not yet available.

Bahrain enacted the *Personal Data Protection Law* (Law No 30 of 2018) (PDPL) in July 2018 which will come into force on 1 August 2019. The legislation is directly influenced by the country's ambitious plans to become a hub for data centres, with Amazon Web Services planning on opening data centres in Bahrain by 2019.

The PDPL aims to be consistent with international practices in the protection of Personal Data and to enhance the attractiveness of Bahrain to foreign investors by providing a clear framework for Processing Personal Data. Indeed, its requirements are heavily based on the GDPR. It includes the protection of individuals' privacy and specific consent requirements for data Processing, as well as the creation of a Personal Data Protection Authority.

By contrast, the PDPL introduces separate and additional provisions not found in the GDPR. One of the most notable is its application not only to Bahraini residents and companies Processing their data, but also individuals not normally residing or working in Bahrain and companies without a place of business in the country, that process Personal Data by using means available in Bahrain. Processing solely used for data transfers is excluded from this third category.

The PDPL will provide individuals with rights in relation to how their Personal Data can be collected, Processed and stored. Conversely, it will impose new obligations on how businesses manage this, including ensuring that Personal Data is processed fairly, that data owners are notified of when their Personal Data is collected and processed and that data owners can exercise their rights directly with the businesses. The PDPL also imposes new obligations upon businesses to ensure that the Personal Data they collect is kept secure.

Bahrain also currently has a number of laws with limited provisions relating to data protection, including the *Bahraini Constitution*, the *Penal Code* (Amiri Decree No 15 of 1976), the *E-Transactions Law* (Legislative Decree No 54 of 2018), the *Telecommunications Law* (Legislative Decree No 48 of 2002) and the *Cyber Crimes Law* (Law No 60 of 2014).

As it currently stands, the PDPL will only will supersede any existing national law with contradictory provisions. It is unclear whether certain sectors will more to further modernise sectoral laws in light of the PDPL or to provide for certain sectoral carve outs.

	GDPR	PDPL	General Observations
Principles of Data Processing	<p>Lawfulness, fairness, transparency Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. (Article 5(1)(a))</p> <p>Specified purposes Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. (Article 5(1)(b))</p> <p>Data minimisation Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. (Article 5(1)(c))</p> <p>Accuracy Personal Data must be accurate and, where necessary, kept up to date. (Article 5(1)(d))</p> <p>Storage limitation Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. (Article 5(1)(e))</p> <p>Integrity and confidentiality Personal Data must be processed in a way 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. (Article 5(1)(f))</p> <p>Accountability The controller shall be responsible for and be able to demonstrate compliance with all the above principles. (Article 5(2))</p> <p>Lawful bases The legal bases under which Personal Data may be processed are</p>	<p>Just and legal Processing of Personal Data must be just and legal. (Article 3(1))</p> <p>Specified purposes Personal Data must be collected for legal, specific and clear purposes and must not be further processed in ways incompatible with those purposes. (Article 3(2))</p> <p>Data minimisation The collection and Processing of Personal Data shall be sufficient, relevant and non-excessive, taking into consideration the purposes for which they are processed. (Article 3(3))</p> <p>Data minimisation Personal Data shall be correct, concise and updated when requested by the Data Subject. (Article 3(4))</p> <p>Storage limitation Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. (Article 3(5))</p>	<p>Basis The new PDPL is consistent with international practices in the protection of Personal Data and broadly aligns with the GDPR. The PDPL has extraterritorial effect, places certain restrictions on cross-border data transfers, and mandates that data managers (the equivalent of data controllers) must enter into written contracts with data processors.</p> <p>There are however also some notable differences, as set out below:</p> <ul style="list-style-type: none"> • There is no mandatory breach notification provision as under the GDPR. • The law carries criminal penalties, including imprisonment, for violations of certain provisions, one of which is those on cross-border data transfers. • Data Protection Supervisors (the equivalent of DPOs), must be accredited by, and registered with, the Personal Data Protection Authority (PDPA). • Data Subjects have the right to object to Processing that may cause the data owner or any third party a material or moral damage. Such a right is not found in the GDPR. <p>Looking forward The PDPL is set to come into force in August 2019. However, it must be noted that no data protection regulator tasked with supervision and enforcement under the law has yet been established.</p>

GDPR		PDPL	General Observations
	<ul style="list-style-type: none"> with the freely given, specific, informed and unambiguous consent of the Data Subject; where necessary for the performance of a contract to which the Data Subject is party; where necessary to comply with a legal obligation to which the controller is subject; where necessary to protect the vital interests of the Data Subject or another person; where 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 where necessary for the purposes of the legitimate interests of the controller or a third party. (Article 6(1)) 		
Data Controller and Data Processor Obligations	<p>General principles The controller is responsible for compliance with the principles listed in Article 5 (as set out above). The controller must have regard to 'data protection by design and by default' throughout their Processing activities.</p> <p>Lawful processing The controller must carry only process Personal Data under one of the conditions laid out in Article 6 and for special categories of Personal Data those laid out in Article 9.</p> <p>Sensitive personal data The Processing of sensitive Personal Data is prohibited, unless the:</p> <ul style="list-style-type: none"> Data Subject has given explicit consent. (Article 9(2)(a)) Processing is necessary in the context of employment law, or laws relating to social security and social protection. (Article 9(2)(b)) Processing is necessary to protect vital interests of the Data Subject (or another person). (Article 9(2)(c)) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit 	<p>Data manager 'Data Manager' is the equivalent of the GDPR term 'Data Controller'. This is defined as 'any person who individually or collectively with any other party determines the purposes and means of Processing Personal Data'. (Article 1)</p> <p>General principles The data manager must process Personal Data in compliance with the Data Quality Controls set out in Article 3 (as listed above).</p> <p>Lawful processing The data manager must only process Personal Data with the consent of the data owner, or under one of the conditions laid out in Article 4 ('general conditions of legal Processing'):</p> <ul style="list-style-type: none"> For the execution of a contract; (Article 4(1)) To take steps under instructions from the data owner for entering into a contract; (Article 4(2)) For execution of an obligation under law; (Article 4(2)) To protect the best interests of the data owner. (Article 4(4)) For the legitimate interests of the data manager or any third party, unless this contradicts the rights of the data owner. (Article 4(5)) 	<p>Bahrain, being based on international best practices and broadly aligned with the GDPR, largely mirrors the GDPR in terms of obligations imposed on Data Controllers and Data Processors.</p> <p>The obligations in respect of appointing a Data Processor do not appear as onerous under the PDPL as they do under Article 28, GDPR.</p>

GDPR	PDPL	General Observations
<p>body with a political, philosophical, religious or trade union aim. (Article 9(2)(d))</p> <ul style="list-style-type: none"> Processing relates to Personal Data which are manifestly made public by the Data Subject. (Article 9(2)(e)) Processing is necessary for the establishment, exercise or defence of legal claims. (Article 9(2)(f)) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law. (Article 9(2)(g)) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional. (Article 9(2)(h)) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law. (Article 9(2)(i)) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. (Article 9(2)(j)) <p>Technical & organisational measures The controller is responsible for implementing appropriate technical and organisational measures to ensure and demonstrate that its Processing activities are compliant with the requirements of the GDPR. (Article 32)</p> <p>Data subject rights The controller must demonstrate the Data Subject's consent to Processing their Personal Data. The consent must be clearly presented and easily distinguished from other matters, in an intelligible and easily accessible form.</p>	<p>The data manager must only process sensitive Personal Data with the consent of the data owner, or under one of the conditions laid out in Article 5 ('conditions for sensitive Personal Data Processing'), which include where the Processing is necessary:</p> <ul style="list-style-type: none"> to enable the Data Manager to carry out his employment law rights and obligations. for the protection of any person if the Data Owner is not legally able to give his consent thereon. to exercise any of the procedures of claims of legal rights or the defence thereof. for the purposes of preventive medicine, medical diagnosis, provision of healthcare, treatment or management of healthcare services by a person licensed to exercise any of the medical practices or any person legally bound to maintain confidentiality. for the activities of associations, unions and other non-profit organisations. by a competent public entity to the extent required by the performance of the tasks entrusted to it under the law. to ascertain equal opportunities or treatment of the society's individuals who are of different races or ethnic origins, provided that the appropriate guarantees of the rights and freedoms of Data Owners prescribed by the law are taken in consideration. (Article 5(1) – (8)) <p>Article 7 also states that it is prohibited to process Personal Data related to criminal cases, unless one of the listed exclusions apply. (Article 7)</p> <p>Technical & organisational measures The data manager is responsible for implementing appropriate technical and organisational measures to ensure that Personal Data is protected from unauthorised or unintended destruction, accidental loss, or any unauthorised change, disclosure, access, or any other type of Processing.</p>	

GDPR	PDPL	General Observations
<p>The consent must be able to be withdrawn at any time. (Article 24)</p> <p>The controller must make reasonable efforts to verify parental consent (when the child is under 16, although in some members states may be as young as 13).</p> <p>Choosing a data processor</p> <p>The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of this Regulation and ensure the protection of the rights of the Data Subject.</p> <p>Processing by a processor shall be governed by a contract or other legal act. (Article 28)</p> <p>Notifications</p> <p>In the case of a Personal Data breach, the controller must notify the supervisory authority of the breach. This must be done without due delay and, where feasible, not later than 72 hours after having become aware of it. (Article 33)</p> <p>Record keeping</p> <p>Each controller must maintain a record of its Processing activities. (Article 30)</p> <p>Appoint a representative</p> <p>The controller must appoint an EU representative in certain situations. (Article 27)</p> <p>Appoint a DPO</p> <p>The controller must appoint a Data Protection Officer (DPO) in certain situations. (Article 37(1))</p>	<p>The data manager must record the technical and organisational measures in place and make these available for review by the parties concerned, the regulator, the Data Manager and the Data Processor. (Article 8(1))</p> <p>Choosing a data processor</p> <p>The data manager shall only use processors providing sufficient guarantees to implement appropriate technical and organisational measures. The data manager shall take reasonable steps to ensure the processor is complying with such. (Article 8(3)(A))</p> <p>Processing by a processor must be governed by a written contract between the data manager and processors which includes the following:</p> <ul style="list-style-type: none"> • That the processor will not commence any Processing unless on the instructions of the data manager. • That the data processor shall comply with the obligations of the data manager in respect of security and confidentiality. (Article 8(3)(B)) <p>Confidentiality</p> <p>The data manager must not disclose any Personal Data unless with the approval of the data owner or for execution of a judicial order. (Article 9(1))</p> <p>The data manager must not process Personal Data except in compliance with the Data Protection Law. (Article 9(2))</p> <p>Data Protection Supervisor</p> <p>Article 10(4) states that the board of directors of the Personal Data Protection Authority (PDPA) may issue decisions obliging certain categories of data managers to appoint a 'data protection supervisor'.</p>	

GDPR	PDPL	General Observations
	<p>The data manager must notify the PDPA of the appointment of a data protection supervisor within 3 working days from its date. (Article 10))</p> <p>Cross-border data transfers The data manager must not transfer any Personal Data outside of Bahrain except in compliance with the rules listed in Articles 12 and 13. (See below section on cross-border data transfers).</p> <p>Notification The data manager must serve the PDPA a notification before the commencement of Processing any Personal Data, except in the case of an exemption. (Article 14)</p> <p>Automated processing and monitoring Certain automated Processing must not be carried out without prior written consent from the PDPA. (Article 15(1)(A) – (E))</p> <p>Transparency Where Personal Data are obtained directly from the Data Subject, the data manager must provide the following information:</p> <ul style="list-style-type: none"> • Full name, address and profession of the data manager. • Purposes of Processing • Any other important information including names and categories of data recipients, whether providing the information is mandatory, any consequences of withholding the information, statement of Data Subjects rights, whether the data will be used for direct marketing. (Article 17(1)) <p>Where Personal Data is not obtained from the Data Subject, the data manager must provide the following information:</p> <ul style="list-style-type: none"> • The same information as stated above when received directly from Data Subjects; 	

GDPR		PDPL	General Observations
		<ul style="list-style-type: none"> The purposes for which the data is collected; Any other important information that will make the Processing fair to the Data Subject, including the information listed above, the categories of data, and the source of the data. (Article 17(2)) <p>Data subject rights The data manager must respond to requests from Data Subjects (as detailed below in the 'Data Subject rights' section). (Articles 18-23)</p>	
Data Subject Rights	<p>Transparent communication In order to ensure that Personal Data are processed fairly and lawfully, controllers must provide certain minimum information to Data Subjects, regarding the collection and further Processing of their Personal Data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. (Articles 5(1)(a), 12-14)</p> <p>Data subject rights Data controllers have a legal obligation to give effect to the rights of Data Subjects. (Article 12(2))</p> <p>Identifying data subjects Data controllers must not refuse to give effect to the rights of a Data Subject unless the controller cannot identify the Data Subject. The controller must use all reasonable efforts to verify the identity of Data Subjects. Where the controller has reasonable doubts as to the identity of the Data Subject, the controller may request the provision of additional information necessary to confirm the identity of the Data Subject, but is not required to do so. (Article 12(2), (6))</p> <p>Time limits A controller must, within one month of receiving a request made under those rights, provide any requested information in relation to any of the rights of Data Subjects. If the controller fails to meet this deadline, the</p>	<p>Right to access Data Subjects have the right to know what Personal Data is being processed. Requests can be made to data managers and data managers must respond to such requests within 15 days from the application date. The data manager must respond with the following:</p> <ul style="list-style-type: none"> what Personal Data is being processed; the source of the data; the purpose of the Processing; the names and categories of data recipients; and if the Processing involves automated decision making, an explanation of how this will be used. (Article 18(1)) <p>Right to object to direct marketing The data manager must notify the Data Subject that he has the right to object to direct marketing. (Article 19)</p> <p>Right to object to processing that may cause material or moral damage Data Subject may request that Processing is stopped if such Processing will cause them or a third party material or moral damage which is material and unjustifiable. Such a request must be fulfilled within 10 working days of being received. (Article 21)</p>	The PDPL largely mirrors the GDPR in terms of Data Subject rights.

GDPR	PDPL	General Observations
<p>Data Subject may complain to the relevant DPSA and may seek a judicial remedy. Where a controller receives large numbers of requests, or especially complex requests, the time limit may be extended by a maximum of two further months. (Article 12(3) - (4))</p> <p>Basic information Data Subjects have the right to be provided with information on the identity of the controller, the reasons for Processing their Personal Data and other relevant information necessary to ensure the fair and transparent Processing of Personal Data. (Articles 13 and 14)</p> <p>Right of access Data Subjects have the right to obtain the following:</p> <ul style="list-style-type: none"> • confirmation of whether, and where, the controller is Processing their Personal Data; • information about the purposes of the Processing; • information about the categories of data being processed; • information about the categories of recipients with whom the data may be shared; • information about the period for which the data will be stored (or the criteria used to determine that period); • information about the existence of the rights to erasure, to rectification, to restriction of Processing and to object to Processing; • information about the existence of the right to complain to the DPSA; • where the data were not collected from the Data Subject, information as to the source of the data; and • information about the existence of, and an explanation of the logic involved in any automated Processing that has a significant effect on Data Subjects; and • Data Subjects may request a copy of the Personal Data being processed. (Article 15) <p>Access fees Data controllers must give effect to the rights of access, rectification, erasure and the right to object, free of</p>	<p>Automated decision making Data Subjects have the right to insist that decisions made regarding performance at work, financial position, credit risk/rating, or behaviour on the basis of automated Processing are made by other non-automated means. (Article 22)</p> <p>Right to correction, suspension or deletion Data Subjects have the right to request that their Personal Data is corrected or deleted in certain circumstances as well as the right to request that Processing of their Personal Data is suspended. The data manager must respond to any request within 15 days. (Article 23)</p> <p>Withdraw consent Data Subjects have the right to submit an application to withdraw their consent at any time. (Article 24(3))</p> <p>Submit complaints Any Data Subject may submit a complaint to the PDPA if he believes there has been a breach of the provisions of the Data Protection Law. (Article 25)</p>	

GDPR	PDPL	General Observations
	<p>charge. The controller may charge a reasonable fee for "repetitive requests", "manifestly unfounded or excessive requests" or "further copies". (Articles 12(5), 15(3), (4))</p> <p>Rectification Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data Subjects have the right to rectification of inaccurate Personal Data. (Articles 5(1)(d), 16)</p> <p>Erase Data Subjects have the right to erasure of Personal Data if:</p> <ul style="list-style-type: none"> • the data are no longer needed for their original purpose (and no new lawful purpose exists); • the lawful basis for the Processing is the Data Subject's consent, the Data Subject withdraws that consent, and no other lawful ground exists; • the Data Subject exercises the right to object, and the controller has no overriding grounds for continuing the Processing; • the data have been processed unlawfully; or • erasure is necessary for compliance with EU law or the national law of the relevant Member State. (Article 17) <p>Restrict processing Data Subjects have the right to restrict the Processing of Personal Data (meaning that the data may only be held by the controller, and may only be used for limited purposes) if:</p> <ul style="list-style-type: none"> • the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); • the Processing is unlawful and the Data Subject requests restriction (as opposed to exercising the right to erasure); • the controller no longer needs the data for their original purpose, but the data are still required by the 	

GDPR	PDPL	General Observations
	<p>controller to establish, exercise or defend legal rights; or</p> <ul style="list-style-type: none"> • if verification of overriding grounds is pending, in the context of an erasure request. (Article 18) <p>Portability Data Subjects have a right to:</p> <ul style="list-style-type: none"> • receive a copy of their Personal Data in a structured, commonly used, machine-readable format that supports re-use; • transfer their Personal Data from one controller to another; • store their Personal Data for further personal use on a private device; and • have their Personal Data transmitted directly between controllers without hindrance. (Article 20) <p>Object to processing Data Subjects have the right to object, on grounds relating to their particular situation, to the Processing of Personal Data, where the basis for that Processing is either:</p> <ul style="list-style-type: none"> • public interest; or • legitimate interests of the controller. <p>The controller must cease such Processing unless the controller:</p> <ul style="list-style-type: none"> • demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject; or • requires the data in order to establish, exercise or defend legal rights. (Article 21) <p>Where Personal Data are processed for scientific and historical research purposes or statistical purposes, the Data Subject has the right to object, unless the Processing is necessary for the performance of a task carried out for reasons of public interest. (Articles 21(6), 83(1))</p>	

GDPR		PDPL	General Observations
	<p>Object to direct marketing Data Subjects have the right to object to the Processing of Personal Data for the purpose of direct marketing, including profiling. (Article 21(2) – (3))</p> <p>Duty to inform of right to object The right to object to Processing of Personal Data noted above must be communicated to the Data Subject no later than the time of the first communication with the Data Subject. This information should be provided clearly and separately from any other information provided to the Data Subject. (Articles 3(2)(b), 14(2)(c), 15(1)(e), 21(4))</p> <p>Automated processing Data Subjects have the right not to be subject to a decision based solely on automated Processing which significantly affect them (including profiling). Such Processing is permitted where:</p> <ul style="list-style-type: none"> • it is necessary for entering into or performing a contract with the Data Subject provided that appropriate safeguards are in place; • it is authorised by law; or • the Data Subject has explicitly consented and appropriate safeguards are in place. (Article 22) 		
Cross-Border Transfer Rules	<p>General prohibition Cross-Border Personal Data Transfers may only take place if the transfer is made to an Adequate Jurisdiction or the data exporter has implemented a lawful data transfer mechanism (or an exemption or derogation applies). (Articles 44, 45)</p> <p>Adequacy decisions Cross-border data transfers may take place if the third country receives an Adequacy Decision from the EU Commission. (Articles 44, 45)</p> <p>The EU Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe</p>	<p>General prohibition Data managers may not transfer Personal Data outside of Bahrain except in the following cases:</p> <ul style="list-style-type: none"> • The transfer is to a country or territory deemed adequate by the PDPA. (Article 12(1)) • The PDPA has issued a permit for such transfer after deeming the location can provide a sufficient level of protection of the Personal Data given all the circumstances. The permit may be conditional or for a specific term. (Article 12(2)) <p>The Data Subject has consented to the transfer, or any of the other conditions in Article 13 apply. (Article 13)</p>	<p>The rules surrounding cross-border data transfers in Bahrain, being based on based on international practices, mirror to a significant extent those in the GDPR.</p> <p>It is expected that the list of countries deemed adequate by the PDPA will mirror those deemed adequate by the European Commission. No list has been published to-date.</p> <p>NOTE: Under the GDPR, cross-border data transfers may take place on the basis of standard data protection clauses approved by the EU Commission (“Model Clauses”). The current set of Model Clauses are currently</p>

GDPR	PDPL	General Observations
<p>Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the USA (subject to compliance with the terms of the US-EU Privacy Shield).</p> <p>Public authorities Cross-border data transfers between public authorities may take place under agreements between public authorities, which do not require any specific authorisation from a DPSA. (Articles 46(2)(a), 46(3)(b))</p> <p>Binding Corporate Rules Cross-Border Data Transfer within a corporate group may take place on the basis of Binding Corporate Rules ("BCRs"). BCRs require approval from DPSAs, but approved, individual transfers made under the BCRs do not require further approval. (Articles 4(20) 46(2)(b), 47)</p> <p>Model clauses Cross-border data transfers may take place on the basis of the Model Clauses entered into between the data exporter and data recipient. Existing Model Clauses implemented under the 1995 Directive remain valid until amended, replaced or repealed under the GDPR. (Articles 28(6)-(8), 46(2)(c), 57(1)(j), (r), 93(2))</p> <p>Other mechanisms Cross-border data transfers may take place on the basis, <i>inter alia</i>, of:</p> <ul style="list-style-type: none"> • standard data protection clauses adopted by one or more DPSAs under the GDPR. (Articles 46(2)(d), 64(1)(d), 57(1)(j), (r), 93(2)) • an approved code of conduct, together with binding and enforceable commitments to provide appropriate safeguards. (Articles 40, 41, 46(2)(e)) • certifications together with binding and enforceable commitments of the data importer to apply the certification to the transferred data. (Articles 42, 43, 46(2)(f)) • ad hoc clauses conforming to the GDPR and approved by the relevant DPSA. (Articles 46(3)(a), (4), 63)) 		<p>being challenged as a form of appropriate data transfer mechanism; therefore their future is uncertain.</p> <p>In January 2019, the Irish Supreme Court (as part of the <i>Schrems v Facebook</i> litigation) heard an appeal by Facebook over a decision of the Irish High Court to refer a number of questions to the Court of Justice of the EU ("CJEU") regarding the validity of this data transfer mechanism. The Supreme Court will publish its decision in due course. If Facebook is unsuccessful in its appeal, the CJEU will rule on these questions, which may result in a declaration that the Model Clauses are no longer valid as a transfer mechanism.</p>

GDPR		PDPL	General Observations
	<ul style="list-style-type: none"> administrative arrangements between public authorities (e.g., MOUs) subject DPSA approval. (Articles 46(3)(b), (4), 63) <p>Derogations Cross-border data transfers may be made on the basis, <i>inter alia</i>, that:</p> <ul style="list-style-type: none"> the Data Subject explicitly consents having been informed of the possible risks of such transfer. (Article 49(1)(a), (3)) the performance of a contract between the Data Subject and the controller. (Article 49(1)(b), (3)) it is necessary for the purposes of performing or concluding a contract in the interests of the Data Subject. (Article 49(1)(c), (3)) the transfer is necessary for important reasons of public interest. (Article 49(1)(d), (4)) it is necessary for the purposes of legal proceedings, or obtaining legal advice. (Article 49(1)(e)) the transfer is necessary in order to protect the vital interests of the Data Subject, where the Data Subject is incapable of giving consent. (Article 49(1)(f)) the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by those of the individual subject to informing the relevant DPSA and the Data Subjects. (Article 49(1), (3), (6)) 		
Personal Data Security	<p>Security Data controllers must implement appropriate technical and organisational security measures to protect Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.</p> <p>Depending on the nature of the Processing, these measures may include:</p> <ul style="list-style-type: none"> encryption of the Personal Data; on-going reviews of security measures; redundancy and back-up facilities; and 	<p>Technical & organisational measures The data manager shall apply technical and organisational measures to protect Personal Data from unintended or unauthorised destruction, accidental loss, or any unauthorised change, disclosure, access, or any other type of Processing. (Article 8(1))</p> <p>These technical and organisational measures shall be recorded and made available for review by the concerned persons, the PDPA, data manager and processor. (Article 8(1))</p>	Being based on international practices and broadly aligning with the GDPR, the PDPL places strict data security obligations on data managers.

GDPR		PDPL	General Observations
	<ul style="list-style-type: none"> regular security testing. (Article 32) 	<p>Data managers must consider the following when selecting data processors:</p> <ul style="list-style-type: none"> That they offer sufficient guarantees in respect of technical and organisational measures to protect the Personal Data. That they sign a written contract stating the data processor shall comply with the security and confidentiality obligations. (Article 8(3)) <p>Confidentiality Data managers must not disclose any Personal Data without the Data Subjects consent or for execution of a judicial order. (Article 9)</p>	
Administrative Fines and Regulatory Sanctions	<p>Judicial remedies Data Subjects have the right to an effective judicial remedy against:</p> <ul style="list-style-type: none"> decisions of a DPSA concerning them; any failure by a DPSA to deal with, or respond to, a complaint within three months; and any unlawful Processing of their Personal Data by a controller or processor. (Article 78-79) <p>Compensation & liability A Data Subject who has suffered harm as a result of the unlawful Processing of his or her Personal Data has the right to receive compensation from the controller or processor for the harm suffered:</p> <ul style="list-style-type: none"> Any controller involved in the Processing is liable for the harm caused. A processor is liable for the harm caused by any of its (or its sub-processor's) Processing activities that are not in compliance with its obligations under the GDPR, or are in breach of the controller's instructions. To ensure effective compensation, each controller or processor will be held liable for the entirety of the harm 	<p>Penalties Imprisonment for a period not exceeding 1 year and/or a fine of not less than 1,000 Dinar and not exceeding 20,000 dinar for any person who:</p> <ul style="list-style-type: none"> Processes sensitive personal information in violation of article 5; Transfers Personal Data outside of Bahrain in violation of Article 12 and 13. Processes Personal Data without notifying the PDPA in violation of Article 14. Fails to notify the PDPA of any change made in violation of Article 14. Processes Personal Data without prior authorisation from the PDPA in violation of Article 15. Submits to the PDPA false or misleading information. Withholds from the PDPA any data, information, records or misleading data. Hinders or suspends the work of the PDPA. Discloses any data or information which he is allowed to have access to due to his job which he uses for his own benefit or the benefit of others unreasonably and in violation of the PDPL. (Article 58(1)) 	<p>Whereas the remedies and sanctions available under the PDPL are comparatively low, the remedies and sanctions available to DPSAs under the GDPR are significantly greater.</p> <p>Under the GDPR, DPSAs are considered to have more significant enforcement powers.</p>

GDPR	PDPL	General Observations
	<p>caused, if they are involved in the same Processing and responsible for that harm. (Article 82(1)-(2), (4))</p> <p>Joint-controller liability Data Subjects are entitled to enforce their rights against any of the joint controllers. Each joint controller is liable for the entirety of the damage, although national law may apportion liability between them. If one joint controller has paid full compensation, it may then bring proceedings against the other joint controllers to recover their portions of the damages. (Article 26(3), 82(3)-(5))</p> <p>Exemptions from liability A controller or processor is exempt from liability if it proves that it is not responsible for the event giving rise to the harm. There is no mention of force majeure events. (Article 82(3))</p> <p>Administrative fines The maximum fine that can be imposed for serious infringements of the GDPR is the greater of €20 million or 4% of an undertaking's worldwide turnover for the preceding financial year. (Article 83(5) – (6))</p> <p>Fine criteria When deciding whether to impose a fine and deciding on the amount, DPSAs are required to give due regard to a range of issues, including:</p> <ul style="list-style-type: none"> • the nature, gravity and duration of the infringement; • the number of Data Subjects affected and the level of harm suffered by them; • the intentional or negligent character of the infringement; • any action taken by the controller or processor to mitigate the harm; • any relevant previous infringements by the controller or processor; • the degree of co-operation with the relevant DPSA; • whether the infringement was self-reported by the controller or processor; and <p>Legal persons The legal person shall be sentenced to pay a fine as specified for the crime. (Article 59)</p>	

GDPR		PDPL	General Observations
	<ul style="list-style-type: none"> any other aggravating or mitigating factors. (Article 82(3)) 		
Role and Powers of any relevant Data Protection Supervisory Authority	<p>Independence DPSAs must act independently and operate free from all outside influences, including government control. (Article 52)</p> <p>Tasks The tasks of DPSAs include obligations to:</p> <ul style="list-style-type: none"> monitor and enforce the application of the GDPR; promote awareness of the risks, rules, safeguards and rights pertaining to Personal Data (especially in relation to children); advise national and governmental institutions on the application of the GDPR; hear claims brought by Data Subjects or their representatives, and inform Data Subjects of the outcome of such claims; establish requirements for Impact Assessments; encourage the creation of Codes of Conduct and review certifications; authorise Model Clauses and BCRs; keep records of sanctions and enforcement actions; and fulfil "any other tasks related to protection of Personal Data". (Article 55, 57) <p>Powers DPSAs are empowered to oversee enforcement of the GDPR, investigate breaches of the GDPR and bring legal proceedings where necessary. (Article 58)</p>	<p>Personal Data Protection Authority The PDPA will have power to investigate violation of the Data Protection Law on its own, at the request of the Minister, or in response to a complaint. (Article 30)</p> <p>Powers The PDPA can issue orders to stop violations. This includes ordering fines and emergency orders. (Article 30)</p> <p>Civil compensation may be awarded to any individual who has incurred damage as a result of the Processing of their Personal Data by the data manager, or data protection supervisor. (Article 57)</p>	Under the GDPR, DPSAs are considered to have more significant supervisory and enforcement powers compared with the PDPL. To-date, the PDPA has yet to be established under the PDPL.

LEBANON



Lebanon – Executive summary



Privacy and data protection is governed in Lebanon by Law No 81 of 2018 (the “**E-Transactions and Personal Data Law**”) and to a limited extent by the Lebanese Constitution. The Constitution does not explicitly protect the right to privacy but rather protects the inviolability of the home. In addition, the Constitution indirectly guarantees individual liberty and freedom of expression, respectively. Some legal experts have interpreted that these laws could protect the secrecy of all means of communications but this protection is not explicit.

The E-Transactions and Personal Data Law was originally introduced in 2004 but was updated in 2018. However, the framework has been criticised for being weak and somewhat outdated by not reflecting the reality of online data and that the substantive provisions include vague and open-ended requirements. Additionally, experts say that the law fails to adequately protect Lebanese citizens’ and residents’ data by putting in place weak safeguards

and only granting authority to the executive branch of the Lebanese Government.

The E-Transactions and Personal Data Law is not as detailed or comprehensive as the GDPR, primarily as it fails to provide for the establishment of an independent regulatory body in charge of monitoring Personal Data protection. The law also still awaits the enactment of certain implementing decrees/regulations that will help to secure its proper understanding and implementation.

Privacy is also regulated by other various provisions including Law 140 of 1999, the *Banking Secrecy Law* of 3 September 1956 and the *Penal Code*. The recent Right to Access Information Law 2016 “prevents public institutions from providing anyone with private and personal information about Lebanese citizens.” The *Consumer Protection Code* (Law No 659 of 4 February 2005) states that suppliers must not disclose data without the consent of the consumer.

	GDPR	E-Transactions and Personal Data Law	General Observations
Principles of Data Processing	<p>Lawfulness, fairness, transparency Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. (Article 5(1)(a))</p> <p>Specified purposes Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. (Article 5(1)(b))</p> <p>Data minimisation Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. (Article 5(1)(c))</p> <p>Accuracy Personal Data must be accurate and, where necessary, kept up to date. (Article 5(1)(d))</p> <p>Storage limitation Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. (Article 5(1)(e))</p> <p>Integrity and confidentiality Personal Data must be processed in a way 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. (Article 5(1)(f))</p> <p>Accountability The controller shall be responsible for and be able to demonstrate compliance with all the above principles. (Article 5(2))</p> <p>Lawful bases The legal bases under which Personal Data may be processed are:</p>	<p>Specified purposes Personal Data shall be collected faithfully and for legitimate, specific and explicit purposes and shall not be processed for purposes that are not in line with the objectives specified, unless this is related to Processing data for statistical or historical purposes or for scientific research. (Article 87)</p> <p>Data minimisation Personal Data shall be appropriate, not go beyond the stated objectives. (Article 87)</p> <p>Accuracy Personal Data shall be correct and complete and remain on a daily basis as relevant as possible. (Article 87)</p> <p>Storage limitation Retention of Personal Data shall not be legitimate except during the period specified in the declaration of Processing or in the decision authorising the same. (Article 90)</p>	<p>The E-Transactions and Personal Data Law lacks the depth and comprehensiveness of the GDPR in terms of fleshing out the core principles of data protection. This appears to suggest that the level of protection afforded to Lebanese citizens falls short of that provided to Data Subjects by the GDPR.</p> <p>Of particular note is the absence of reference to the very essence of the GDPR, the principles of transparency and accountability. The framework has been criticised for being weak and somewhat outdated by not reflecting the reality of online data and that the substantive provisions include vague and open-ended requirements.</p>

GDPR		E-Transactions and Personal Data Law	General Observations
	<ul style="list-style-type: none"> with the freely given, specific, informed and unambiguous consent of the Data Subject; where necessary for the performance of a contract to which the Data Subject is party; where necessary to comply with a legal obligation to which the controller is subject; where necessary to protect the vital interests of the Data Subject or another person; where 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 where necessary for the purposes of the legitimate interests of the controller or a third party. (Article 6(1)) 		
Data Controller and Data Processor Obligations	<p>General principles The controller is responsible for compliance with the principles listed in Article 5 (as set out above). The controller must have regard to 'data protection by design and by default' throughout their Processing activities.</p> <p>Lawful processing The controller must carry only process Personal Data under one of the conditions laid out in Article 6 and for special categories of Personal Data those laid out in Article 9.</p> <p>Sensitive personal data The Processing of sensitive Personal Data is prohibited, unless the:</p> <ul style="list-style-type: none"> Data Subject has given explicit consent. (Article 9(2)(a)) Processing is necessary in the context of employment law, or laws relating to social security and social protection. (Article 9(2)(b)) Processing is necessary to protect vital interests of the Data Subject (or another person). (Article 9(2)(c)) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit 	<p>Processing permit Any organisation wishing to process Personal Data must apply for a permit from the Ministry of Economy and Trade (MET). (Article 95)</p> <p>However, a permit shall not be required where processed:</p> <ul style="list-style-type: none"> by a common rights officer; for book-keeping by Non-Profit Organizations of the members and clients thereof within the scope of their normal and legal exercise of their functions; for the keeping of dedicated records, under legal or regulatory provisions, in order to inform the public; by educational institutions for educational or administrative purposes of the said institutions; by parties or members of the institutions, commercial companies, trade unions, associations and self-employed persons, within limits and for the needs of exercising their activities in a legal manner; by clients and customers of institutions, commercial companies, trade unions, associations and self-employed persons, within limits and for the needs of exercising their activities in a legal manner. (Article 94(1) - (7)) 	<p>Unlike the GDPR, the E-Transactions and Personal Data Law requires organisations to obtain permits from the MET in order to be allowed to process Personal Data.</p> <p>In addition, there is no requirement under the E-Transactions and Personal Data Law to notify any data-related incident to a relevant regulator or the Data Subject.</p> <p>Of note is that the Transactions and Personal Data Law contains no provisions similar to Article 28, GDPR governing the use of data processors and sub-processors.</p>

GDPR	E-Transactions and Personal Data Law	General Observations
	<p>body with a political, philosophical, religious or trade union aim. (Article 9(2)(d))</p> <ul style="list-style-type: none"> Processing relates to Personal Data which are manifestly made public by the Data Subject. (Article 9(2)(e)) Processing is necessary for the establishment, exercise or defence of legal claims. (Article 9(2)(f)) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law. (Article 9(2)(g)) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional. (Article 9(2)(h)) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law. (Article 9(2)(i)) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. (Article 9(2)(j)) <p>Technical & organisational measures The controller is responsible for implementing appropriate technical and organisational measures to ensure and demonstrate that its Processing activities are compliant with the requirements of the GDPR. (Article 32)</p> <p>Data subject rights The controller must demonstrate the Data Subject's consent to Processing their Personal Data. The consent must be clearly presented and easily distinguished from other matters, in an intelligible and easily accessible form.</p> <p>Security A Personal Data Processing officer shall take all measures, in light of the nature of the data and the risks resulting from Processing thereof, in order to ensure the integrity and security of the data and to protect the same against being distorted, damaged or accessed by unauthorised persons. (Article 93)</p> <p>Note: There is no definition of a Personal Data Processing officer under the law nor is there any details of when one is required. There are also details concerning regulation and enforcement for the conduct of data Processing officers.</p>	

GDPR		E-Transactions and Personal Data Law	General Observations
	<p>The consent must be able to be withdrawn at any time. (Article 24)</p> <p>The controller must make reasonable efforts to verify parental consent (when the child is under 16, although in some members states may be as young as 13).</p> <p>Choosing a data processor The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of this Regulation and ensure the protection of the rights of the Data Subject.</p> <p>Processing by a processor shall be governed by a contract or other legal act. (Article 28)</p> <p>Notifications In the case of a Personal Data breach, the controller must notify the supervisory authority of the breach. This must be done without due delay and, where feasible, not later than 72 hours after having become aware of it. (Article 33)</p> <p>Record keeping Each controller must maintain a record of its Processing activities. (Article 30)</p> <p>Appoint a representative The controller must appoint an EU representative in certain situations. (Article 27)</p> <p>Appoint a DPO The controller must appoint a Data Protection Officer (DPO) in certain situations. (Article 37(1))</p>		
Data Subject Rights	<p>Transparent communication In order to ensure that Personal Data are processed fairly and lawfully, controllers must provide certain minimum information to Data Subjects, regarding the collection and further Processing of their Personal Data. Such</p>	<p>Basic information The Personal Data Processing officer shall inform Data Subjects of the following by way of an explicit and clear statement:</p>	<p>In comparison to the GDPR, the E-Transactions and Personal Data Law has been criticised for failing to adequately protect Lebanese citizens' and residents' data by putting in place weak safeguards. Indeed the law is light on substantive Data Subject rights.</p>

GDPR	E-Transactions and Personal Data Law	General Observations
<p>information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. (Articles 5(1)(a), 12-14)</p> <p>Data subject rights Data controllers have a legal obligation to give effect to the rights of Data Subjects. (Article 12(2))</p> <p>Identifying data subjects Data controllers must not refuse to give effect to the rights of a Data Subject unless the controller cannot identify the Data Subject. The controller must use all reasonable efforts to verify the identity of Data Subjects. Where the controller has reasonable doubts as to the identity of the Data Subject, the controller may request the provision of additional information necessary to confirm the identity of the Data Subject, but is not required to do so. (Article 12(2), (6))</p> <p>Time limits A controller must, within one month of receiving a request made under those rights, provide any requested information in relation to any of the rights of Data Subjects. If the controller fails to meet this deadline, the Data Subject may complain to the relevant DPSA and may seek a judicial remedy. Where a controller receives large numbers of requests, or especially complex requests, the time limit may be extended by a maximum of two further months. (Article 12(3) - (4))</p> <p>Basic information Data Subjects have the right to be provided with information on the identity of the controller, the reasons for Processing their Personal Data and other relevant information necessary to ensure the fair and transparent Processing of Personal Data. (Articles 13 and 14)</p> <p>Right of access Data Subjects have the right to obtain the following:</p> <ul style="list-style-type: none"> confirmation of whether, and where, the controller is Processing their Personal Data; 	<ul style="list-style-type: none"> the identity of the data-Processing officer or the identity of the representative thereof; (Article 88(1)) the objectives of the Processing; (Article 88(2)) the mandatory or optional nature of answering the questions raised; (Article 88(3)) the consequences of non-response; (Article 88(4)) persons to whom the data is to be sent; (Article 88(5)) the right to access and correct information and the means prepared for the same. (Article 88(6)) <p>When Personal Data is not collected from the person concerned, the data processing officer shall inform them personally and explicitly of:</p> <ul style="list-style-type: none"> the content of the data; the objectives of Processing the right to object to conducting the Processing. (Article 89) <p>Object to processing Data Subjects have the right to object, for legitimate reasons, to the collection and Processing of their Personal Data, including the collection and Processing for the purpose of commercial promotion save for where such Processing is being carried out:</p> <ul style="list-style-type: none"> under a legal obligation to which the data protection officer is subject; and/or where the Data Subject has agreed to the Processing of their Personal Data. (Article 92(1), (2)) <p>Right to enquire Data Subjects have the right to inquire from the data Processing officer about the Processing of the Personal Data in order to determine whether his/her data is being Processed or not. (Article 99)</p> <p>Right of access The Personal Data Processing officer shall provide the Data Subject with a copy of their Personal Data at their request by way of an understandable copy. (Article 99)</p>	

GDPR	E-Transactions and Personal Data Law	General Observations
	<ul style="list-style-type: none"> information about the purposes of the Processing; information about the categories of data being processed; information about the categories of recipients with whom the data may be shared; information about the period for which the data will be stored (or the criteria used to determine that period); information about the existence of the rights to erasure, to rectification, to restriction of Processing and to object to Processing; information about the existence of the right to complain to the DPSA; where the data were not collected from the Data Subject, information as to the source of the data; and information about the existence of, and an explanation of the logic involved in any automated Processing that has a significant effect on Data Subjects; and Data Subjects may request a copy of the Personal Data being processed. (Article 15) <p>Access fees Data controllers must give effect to the rights of access, rectification, erasure and the right to object, free of charge. The controller may charge a reasonable fee for "repetitive requests", "manifestly unfounded or excessive requests" or "further copies". (Articles 12(5), 15(3), (4))</p> <p>Rectification Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data Subjects have the right to rectification of inaccurate Personal Data. (Articles 5(1)(d), 16)</p> <p>Erasure Data Subjects have the right to erasure of Personal Data if:</p> <ul style="list-style-type: none"> the data are no longer needed for their original purpose (and no new lawful purpose exists); <p>Access fees The Personal Data Processing officer may receive a payment for an access request provided that the payment shall not exceed the cost of copying. (Article 100)</p> <p>Additional Information Data Subjects may also request the data Processing officer to hand over the following additional information:</p> <ul style="list-style-type: none"> the purposes, categories, source, subject and nature of the Processing, identification of the persons and their categories to whom the Personal Data is being sent or those who can access the same, as well as the timing and purposes of such access. (Article 99) <p>Rectification Data Subjects have the right to ask the data Processing officer to correct any Personal Data being processed where such data is incorrect. (Article 101)</p> <p>Restrict processing Data Subjects have the right to ask the data Processing officer to carry out correcting, completing, updating and erasing Personal Data, which is incorrect, incomplete, ambiguous, expired or incompatible with the purposes of Processing, or the data that are not to be processed, collected, used, saved or transferred. (Article 101)</p> <p>Where any Personal Data that has been subject to a correction request has been sent to a third party, the data Processing officer shall notify the same of the amendments made at the request of the Data Subject. (Article 101)</p> <p>Automated processing Data Subjects have the right to review and object to the information and analysis used in any automated Processing of their Personal Data. (Article 86)</p>	

GDPR	E-Transactions and Personal Data Law	General Observations
	<ul style="list-style-type: none"> the lawful basis for the Processing is the Data Subject's consent, the Data Subject withdraws that consent, and no other lawful ground exists; the Data Subject exercises the right to object, and the controller has no overriding grounds for continuing the Processing; the data have been processed unlawfully; or erasure is necessary for compliance with EU law or the national law of the relevant Member State. (Article 17) <p>Restrict processing Data Subjects have the right to restrict the Processing of Personal Data (meaning that the data may only be held by the controller, and may only be used for limited purposes) if:</p> <ul style="list-style-type: none"> the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); the Processing is unlawful and the Data Subject requests restriction (as opposed to exercising the right to erasure); the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or if verification of overriding grounds is pending, in the context of an erasure request. (Article 18) <p>Portability Data Subjects have a right to:</p> <ul style="list-style-type: none"> receive a copy of their Personal Data in a structured, commonly used, machine-readable format that supports re-use; transfer their Personal Data from one controller to another; store their Personal Data for further personal use on a private device; and have their Personal Data transmitted directly between controllers without hindrance. (Article 20) 	<p>Complaints Data Subjects have the right to resort to the competent courts in order to ensure the exercise of the right of access and correction and to report the compliance of the data protection officer with the law. (Article 102)</p>

GDPR	E-Transactions and Personal Data Law	General Observations
<p>Object to processing Data Subjects have the right to object, on grounds relating to their particular situation, to the Processing of Personal Data, where the basis for that Processing is either:</p> <ul style="list-style-type: none"> • public interest; or • legitimate interests of the controller. <p>The controller must cease such Processing unless the controller:</p> <ul style="list-style-type: none"> • demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject; or • requires the data in order to establish, exercise or defend legal rights. (Article 21) <p>Where Personal Data are processed for scientific and historical research purposes or statistical purposes, the Data Subject has the right to object, unless the Processing is necessary for the performance of a task carried out for reasons of public interest. (Articles 21(6), 83(1))</p> <p>Object to direct marketing Data Subjects have the right to object to the Processing of Personal Data for the purpose of direct marketing, including profiling. (Article 21(2) – (3))</p> <p>Duty to inform of right to object The right to object to Processing of Personal Data noted above must be communicated to the Data Subject no later than the time of the first communication with the Data Subject. This information should be provided clearly and separately from any other information provided to the Data Subject. (Articles 3(2)(b), 14(2)(c), 15(1)(e), 21(4))</p> <p>Automated processing Data Subjects have the right not to be subject to a decision based solely on automated Processing which</p>		

GDPR		E-Transactions and Personal Data Law	General Observations
	<p>significantly affect them (including profiling). Such Processing is permitted where:</p> <ul style="list-style-type: none"> it is necessary for entering into or performing a contract with the Data Subject provided that appropriate safeguards are in place; it is authorised by law; or the Data Subject has explicitly consented and appropriate safeguards are in place. (Article 22) 		
Cross-Border Transfer Rules	<p>General prohibition Cross-Border Personal Data Transfers may only take place if the transfer is made to an Adequate Jurisdiction or the data exporter has implemented a lawful data transfer mechanism (or an exemption or derogation applies). (Articles 44, 45)</p> <p>Adequacy decisions Cross-border data transfers may take place if the third country receives an Adequacy Decision from the EU Commission. (Articles 44, 45)</p> <p>The EU Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the USA (subject to compliance with the terms of the US-EU Privacy Shield).</p> <p>Public authorities Cross-border data transfers between public authorities may take place under agreements between public authorities, which do not require any specific authorisation from a DPSA. (Articles 46(2)(a), 46(3)(b))</p> <p>Binding Corporate Rules Cross-Border Data Transfer within a corporate group may take place on the basis of Binding Corporate Rules ("BCRs"). BCRs require approval from DPSAs, but approved, individual transfers made under the BCRs do not require further approval. (Articles 4(20) 46(2)(b), 47)</p>	<p>The E-transactions and Personal Data Law is silent on cross-border data transfers. However, the general principles of non-disclosure of Personal Data to a third party without a proper lawful basis (under both the Constitution and the Penal Code) would apply here.</p>	<p>The complete absence of any provisions dealing with cross-border personal data transfers is another reason why the E-Transactions and Personal Data Law has been criticised for affording individuals a lesser degree of protection when it comes to the collection, Processing and use of their Personal Data when compared to the GDPR.</p> <p>NOTE: Under the GDPR, cross-border data transfers may take place on the basis of standard data protection clauses approved by the EU Commission ("Model Clauses"). The current set of Model Clauses are currently being challenged as a form of appropriate data transfer mechanism; therefore their future is uncertain.</p> <p>In January 2019, the Irish Supreme Court (as part of the <i>Schrems v Facebook</i> litigation) heard an appeal by Facebook over a decision of the Irish High Court to refer a number of questions to the Court of Justice of the EU ("CJEU") regarding the validity of this data transfer mechanism. The Supreme Court will publish its decision in due course. If Facebook is unsuccessful in its appeal, the CJEU will rule on these questions, which may result in a declaration that the Model Clauses are no longer valid as a transfer mechanism.</p>

GDPR	E-Transactions and Personal Data Law	General Observations
	<p>Model clauses Cross-border data transfers may take place on the basis of the Model Clauses entered into between the data exporter and data recipient. Existing Model Clauses implemented under the 1995 Directive remain valid until amended, replaced or repealed under the GDPR. (Articles 28(6)-(8), 46(2)(c), 57(1)(j), (r), 93(2))</p> <p>Other mechanisms Cross-border data transfers may take place on the basis, <i>inter alia</i>, of:</p> <ul style="list-style-type: none"> • standard data protection clauses adopted by one or more DPSAs under the GDPR. (Articles 46(2)(d), 64(1)(d), 57(1)(j), (r), 93(2)) • an approved code of conduct, together with binding and enforceable commitments to provide appropriate safeguards. (Articles 40, 41, 46(2)(e)) • certifications together with binding and enforceable commitments of the data importer to apply the certification to the transferred data. (Articles 42, 43, 46(2)(f)) • ad hoc clauses conforming to the GDPR and approved by the relevant DPSA. (Articles 46(3)(a), (4), 63)) • administrative arrangements between public authorities (e.g., MOUs) subject DPSA approval. (Articles 46(3)(b), (4), 63) <p>Derogations Cross-border data transfers may be made on the basis, <i>inter alia</i>, that:</p> <ul style="list-style-type: none"> • the Data Subject explicitly consents having been informed of the possible risks of such transfer. (Article 49(1)(a), (3)) • the performance of a contract between the Data Subject and the controller. (Article 49(1)(b), (3)) • it is necessary for the purposes of performing or concluding a contract in the interests of the Data Subject. (Article 49(1)(c), (3)) • the transfer is necessary for important reasons of public interest. (Article 49(1)(d), (4)) 	

GDPR		E-Transactions and Personal Data Law	General Observations
	<ul style="list-style-type: none"> it is necessary for the purposes of legal proceedings, or obtaining legal advice. (Article 49(1)(e)) the transfer is necessary in order to protect the vital interests of the Data Subject, where the Data Subject is incapable of giving consent. (Article 49(1)(f)) the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by those of the individual subject to informing the relevant DPSC and the Data Subjects. (Article 49(1), (3), (6)) 		
Personal Data Security	<p>Security Data controllers must implement appropriate technical and organisational security measures to protect Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.</p> <p>Depending on the nature of the Processing, these measures may include:</p> <ul style="list-style-type: none"> encryption of the Personal Data; on-going reviews of security measures; redundancy and back-up facilities; and regular security testing. (Article 32) 	<p>Security The Personal Data Processing officer shall take all measures, in light of the nature of the data and the risks resulting from Processing thereof, in order to ensure the integrity and security of the data and to protect the same against being distorted, damaged or accessed by unauthorised persons. (Article 93)</p>	There are no specific provisions relating to Personal Data security akin to the GDPR outside the requirement to take all measures to ensure the integrity and security of the data and to protect the same against being distorted, damaged or accessed by unauthorised persons under the E-Transactions and Personal Data Law. This law provides no guidance on what may be included in “all measures”.
Administrative Fines and Regulatory Sanctions	<p>Judicial remedies Data Subjects have the right to an effective judicial remedy against:</p> <ul style="list-style-type: none"> decisions of a DPSC concerning them; any failure by a DPSC to deal with, or respond to, a complaint within three months; and any unlawful Processing of their Personal Data by a controller or processor. (Article 78-79) <p>Compensation & liability A Data Subject who has suffered harm as a result of the unlawful Processing of his or her Personal Data has the right to receive compensation from the controller or processor for the harm suffered:</p>	<p>Administrative fines The following shall be penalised with a fine of between 1million and 30million Lebanese Pounds and imprisonment from 3 months to 3 years:</p> <ul style="list-style-type: none"> anyone who has processed Personal Data without providing a permit or without obtaining a prior license before Processing; anyone who has collected or processed Personal Data in violation of Articles 87 - 93; and anyone who, even if negligently, discloses Personal Data under Processing to unauthorised persons. (Article 106) 	Whilst the E-Transactions and Personal Data Law provides for financial sanctions for violations of its provisions, these are nominal when compared with the GDPR. This is further compounded by the fact that the law fails to provide for the establishment of an independent regulatory body in charge of monitoring and enforcing Personal Data protection.

GDPR	E-Transactions and Personal Data Law	General Observations
	<ul style="list-style-type: none"> Any controller involved in the Processing is liable for the harm caused. A processor is liable for the harm caused by any of its (or its sub-processor's) Processing activities that are not in compliance with its obligations under the GDPR, or are in breach of the controller's instructions. To ensure effective compensation, each controller or processor will be held liable for the entirety of the harm caused, if they are involved in the same Processing and responsible for that harm. (Article 82(1)-(2), (4)) <p>Joint-controller liability Data Subjects are entitled to enforce their rights against any of the joint controllers. Each joint controller is liable for the entirety of the damage, although national law may apportion liability between them. If one joint controller has paid full compensation, it may then bring proceedings against the other joint controllers to recover their portions of the damages. (Article 26(3), 82(3)-(5))</p> <p>Exemptions from liability A controller or processor is exempt from liability if it proves that it is not responsible for the event giving rise to the harm. There is no mention of force majeure events. (Article 82(3))</p> <p>Administrative fines The maximum fine that can be imposed for serious infringements of the GDPR is the greater of €20 million or 4% of an undertaking's worldwide turnover for the preceding financial year. (Article 83(5) – (6))</p> <p>Fine criteria When deciding whether to impose a fine and deciding on the amount, DPSAs are required to give due regard to a range of issues, including:</p> <ul style="list-style-type: none"> the nature, gravity and duration of the infringement; the number of Data Subjects affected and the level of harm suffered by them; 	<p>Any Personal Data Processing officer who refuses to respond within 10 working days or who responds incorrectly or imperfectly to a data access or correction request shall be liable to a fine between 1million and 15million Lebanese Pounds. (Article 107)</p> <p>In the event of repeat breaches by a data protection officer of the law, the penalties and fines provided for in the aforementioned Articles shall be increased by 30-50%. (Article 108)</p>

GDPR		E-Transactions and Personal Data Law	General Observations
	<ul style="list-style-type: none"> the intentional or negligent character of the infringement; any action taken by the controller or processor to mitigate the harm; any relevant previous infringements by the controller or processor; the degree of co-operation with the relevant DPSA; whether the infringement was self-reported by the controller or processor; and any other aggravating or mitigating factors. (Article 82(3)) 		
Role and Powers of any relevant Data Protection Supervisory Authority	<p>Independence DPSAs must act independently and operate free from all outside influences, including government control. (Article 52)</p> <p>Tasks The tasks of DPSAs include obligations to:</p> <ul style="list-style-type: none"> monitor and enforce the application of the GDPR; promote awareness of the risks, rules, safeguards and rights pertaining to Personal Data (especially in relation to children); advise national and governmental institutions on the application of the GDPR; hear claims brought by Data Subjects or their representatives, and inform Data Subjects of the outcome of such claims; establish requirements for Impact Assessments; encourage the creation of Codes of Conduct and review certifications; authorise Model Clauses and BCRs; keep records of sanctions and enforcement actions; and fulfil "any other tasks related to protection of Personal Data". (Article 55, 57) <p>Powers DPSAs are empowered to oversee enforcement of the GDPR, investigate breaches of the GDPR and bring legal proceedings where necessary. (Article 58)</p>	There is no DPSA in Lebanon.	The E-Transactions and Personal Data Law fails to provide for the establishment of an independent regulatory body in charge of monitoring Personal Data protection.

QATAR



Qatar – Executive summary



This jurisdictional overview is based on an unofficial English translation of the Law No 13 of 2016 Concerning Personal Data Protection and the Telecommunications By-Law No. (1) of 2009. The Qatar government does not issue official English translations of the laws of the State of Qatar.

Qatar was the first GCC nation to issue a generally applicable data protection law when it implemented Law No 13 of 2016 Concerning Personal Data Protection (**Qatar Data Protection Law**). In addition, the Qatar Financial Centre ("**QFC**") introduced its own Data Protection Regulations No 6 of 2005 and Data Protection Rules 2005. As the Qatar Data Protection Law does not expressly exclude the QFC from its provisions, it would be prudent to assume that QFC-registered businesses are also subject to its requirements. The Qatar Data Protection Law took effect in 2017 and executive regulations further implementing this law are expected to be passed in 2019.

The Qatar Data Protection Law is modelled on and incorporates familiar concepts from other international privacy frameworks, such as the 1995 Directive (and by extension the GDPR) and mandates that any party who processes Personal Data adhere to the principles of transparency, fairness and respect for human dignity.

The Ministry of Transport and Communications (**MOTC**) is responsible for implementing and enforcing the Qatar Data Protection Law.

The Qatar Data Protection Law applies to Personal Data when this data is:

- processed electronically;
- obtained, collected or extracted in any other way in preparation for electronic Processing; and/or
- processed by combining electronic Processing and traditional Processing

The Qatar Data Protection Law does not extend protection to private Processing of Personal Data or data collected for the purposes of attaining official statistics. The relevant supervising unit for the Qatar Data Protection law (which sits in the MOTC) is not yet fully operational.

In addition, there are several federal and sectoral laws that contain various provisions in relation to privacy and the protection of Personal Data including the *Telecoms Law* (Law No 34 of 2006) and the *Telecoms By-Laws* (Law No 1 of 2009).

	GDPR	Qatar Data Protection Law	Telecoms Law	General Observations
Principles of Data Processing	<p>Lawfulness, fairness, transparency Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. (Article 5(1)(a))</p> <p>Specified purposes Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. (Article 5(1)(b))</p> <p>Data minimisation Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. (Article 5(1)(c))</p> <p>Accuracy Personal Data must be accurate and, where necessary, kept up to date. (Article 5(1)(d))</p> <p>Storage limitation Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. (Article 5(1)(e))</p> <p>Integrity and confidentiality Personal Data must be processed in a way 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. (Article 5(1)(f))</p>	<p>Lawfulness, fairness, transparency Every individual has the right in protecting the privacy of his Personal Data, and the same may not be processed except with transparency, integrity and respect for human dignity and acceptable practices, as per the provisions of this Law. (Article 3)</p> <p>Data minimisation The controller shall verify that the Personal Data collected by or for it is relevant to the legal purposes and sufficient to achieve the same. (Article 10)</p> <p>Accuracy The controller shall verify that the Personal Data are accurate, complete and up to date to meet the legal purposes. (Article 10)</p> <p>Storage limitation The controller may not keep such Personal Data beyond the period necessary for achieving the legal purposes. (Article 10)</p> <p>Honesty, integrity, legitimacy Data controllers must process Personal Data honestly, integrally and legitimately. (Article 8(1))</p> <p>Lawful bases The MOTC may allow controllers to process Personal Data without consent on the following grounds:</p> <ul style="list-style-type: none"> protecting the national and general security. (Article 18(1)) protecting the international relations of the State. (Article 18(2)) protecting the economic or financial interests of the State. (Article 18(3)) 	<p>Lawful basis Service providers shall be responsible to protect the information, any data related to the customer and customers' communications in their custody and must offer the necessary protection, and the service provider must not collect, use, retain or advertise any customer information unless the customer's approval is obtained or as permitted by law. (Article 52)</p> <p>Due regard to privacy Service providers shall operate their telecommunications networks, facilities and related systems with due regard for the privacy rights of their customers. (Article 52)</p> <p>Accuracy Service providers must ensure that all the information submitted is accurate, complete and valid for use. (Article 52)</p> <p>Telecoms by-laws</p> <p>Lawful bases Service Providers shall not intercept, monitor or alter the content of a customer communication, except with the customer's explicit consent or as expressly permitted or required by applicable laws of Qatar. (Article 91, Telecoms By-Laws)</p> <p>A Service Provider shall not, except as permitted or required by law, or with the consent of the person to whom the information relates, collect, use, maintain or disclose customer information for undisclosed or unauthorised purposes. (Article 91, Telecoms By-Laws)</p>	<p>The Qatar Data Protection Law is in the most part influenced by the 1995 Directive. Therefore it is broadly aligned with the GDPR.</p>

GDPR	Qatar Data Protection Law	Telecoms Law	General Observations
	<p>Accountability The controller shall be responsible for and be able to demonstrate compliance with all the above principles. (Article 5(2))</p> <p>Lawful bases The legal bases under which Personal Data may be processed are:</p> <ul style="list-style-type: none"> • with the freely given, specific, informed and unambiguous consent of the Data Subject; • where necessary for the performance of a contract to which the Data Subject is party; • where necessary to comply with a legal obligation to which the controller is subject; • where necessary to protect the vital interests of the Data Subject or another person; • where 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 • where necessary for the purposes of the legitimate interests of the controller or a third party. (Article 6(1)) 	<ul style="list-style-type: none"> • preventing any crime or collecting information about the same or investigating it. (Article 18(4)) • carrying out a task related to public welfare, as per the law. (Article 19(1)) • implementing any legal obligation or order from a competent court. (Article 19(2)) • protecting the vital interests of the individual. (Article 19(3)) • achieving purposes of scientific research for public welfare. (Article 19(4)) • collecting information needed for investigating any crimes, upon an official request from the investigation bodies. (Article 19(5)) <p>Data sharing A Service Provider shall not disclose customer information to any person without the customer's consent, unless disclosure is required or permitted by the General Secretariat in accordance with the applicable laws or regulations of Qatar. (Article 92, Telecoms By-Laws)</p> <p>Confidentiality Service Providers shall take all reasonable steps to ensure the confidentiality of customer communications. (Article 91, Telecoms By-Laws)</p> <p>Accuracy Service Providers shall ensure that customers' information is accurate, complete and updated regularly for the purposes for which it is to be used. (Article 92, Telecoms By-Laws)</p> <p>Legitimacy The Service Provider shall be entitled to use customer information for all legitimate purposes identified in its terms of service, or in accordance with the customer's consent in accordance with legal and constitutional controls. (Article 92, Telecoms By-Laws)</p> <p>Further processing All customer-specific information, and in particular billing-related information, shall be retained and used by a Service Provider only for purposes specifically provided for in the applicable terms of service or other agreed customer terms, or in accordance with any rules or orders made by the General Secretariat, or as otherwise permitted by applicable laws. (Article 92, Telecoms By-Laws)</p>	

	GDPR	Qatar Data Protection Law	Telecoms Law	General Observations
Data Controller and Data Processor Obligations	<p>General principles The controller is responsible for compliance with the principles listed in Article 5 (as set out above).</p> <p>The controller must have regard to 'data protection by design and by default' throughout their Processing activities.</p> <p>Lawful processing The controller must carry only process Personal Data under one of the conditions laid out in Article 6 and for special categories of Personal Data those laid out in Article 9.</p> <p>Sensitive personal data The Processing of sensitive Personal Data is prohibited, unless the:</p> <ul style="list-style-type: none"> • Data Subject has given explicit consent. (Article 9(2)(a)) • Processing is necessary in the context of employment law, or laws relating to social security and social protection. (Article 9(2)(b)) • Processing is necessary to protect vital interests of the Data Subject (or another person). (Article 9(2)(c)) • Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim. (Article 9(2)(d)) • Processing relates to Personal Data which are manifestly made public by the Data Subject. (Article 9(2)(e)) 	<p>Lawful processing The controller shall process Personal Data honestly and legally. (Article 8(1))</p> <p>Sensitive personal data Sensitive Personal Data may not be processed except after obtaining authorisation from the MOTC. (Article 16)</p> <p>The procedure for obtaining this authorisation has not yet been issued (this is likely to be in the form of a Ministerial resolution).</p> <p>Technical & organisational measures The controller shall take the appropriate administrative, technical and material precautions to protect Personal Data as determined by the concerned department. (Article 8(3))</p> <p>Both the controller and processor shall take the required precautions to protect Personal Data from loss, damage, amendment, disclosure, access or use incidentally or illegally. Such precautions shall be suitable for the nature and importance of the Personal Data to be protected. The processor shall advise the controller about any breach/violation to such precautions or any risk that threatens the Personal Data of individuals, whatsoever, as soon as he knows about the same. (Article 13)</p> <p>Privacy by design The controller shall comply with the rules related to design, change, or development of products, systems and services related to Processing Personal Data. (Article 8(2))</p>	<p>Lawful basis Service providers shall be responsible to protect the information, any data related to the customer and customers' communications in their custody and must offer the necessary protection, and the service provider must not collect, use, retain or advertise any customer information unless the customer's approval is obtained or as permitted by law. (Article 52)</p> <p>Protection of customer information Service providers shall operate their telecommunications networks, facilities and related systems with due regard for the privacy rights of their customers. Service providers shall be responsible to protect the information, any data related to the customer and customers' communications in their custody and must offer the necessary protection, and the service provider must not collect, use, retain or advertise any customer information unless the customer's approval is obtained or as permitted by law. (Article 52)</p> <p>Telecoms by-laws</p> <p>General obligations A Service Provider shall be responsible for any records, which are under its custody or control containing customer information and communications. (Article 92, Telecoms By-Laws)</p> <p>Lawful basis Service Providers shall not intercept, monitor or alter the content of a customer communication, except with the customer's explicit consent or as expressly permitted</p>	<p>The Qatar Data Protection Law deviates from the GDPR wherein it states that the Data Subject should be informed before Processing any Personal Data.</p> <p>In contrast, Article 13 of the GDPR states that "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."</p>

GDPR	Qatar Data Protection Law	Telecoms Law	General Observations
<ul style="list-style-type: none">Processing is necessary for the establishment, exercise or defence of legal claims. (Article 9(2)(f))Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law. (Article 9(2)(g))Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional. (Article 9(2)(h))Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law. (Article 9(2)(i))Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. (Article 9(2)(j)) <p>Technical & organisational measures The controller is responsible for implementing appropriate technical and organisational measures to ensure and demonstrate that its Processing activities are compliant with the requirements of the GDPR. (Article 32)</p>	<p>Privacy policies The controller shall abide by the privacy protection policies set by the concerned department and has a resolution issued by the Minister. (Article 8(4))</p> <p>Privacy protection procedures Data controllers must review their privacy protection procedures before incorporating new Processing operations. (Articles 11(1))</p> <p>Choosing a data processor Data controllers must:</p> <ul style="list-style-type: none">determine the processors in-charge of protecting Personal Data;train and familiarise the processors about Personal Data protection;ensure that the processor complies with the instructions, takes the required precautions for protecting Personal Data, and follows up the same in a continuous manner; andupon disclosing or transferring Personal Data to the processor, ensure that such data conforms to the legal purposes and shall be processed according to the provisions of the law. (Articles 11(2), (3), (8), 12) <p>Data subject rights Data controllers must:</p> <ul style="list-style-type: none">set internal rules for receiving and studying complaints, data access requests, data correction or deletion requests, and make the same available to individuals; anduse technologies to enable the individuals to practice their right in getting access to the Personal Data.	<p>or required by applicable laws of the State of Qatar. (Article 91, Telecoms By-Laws)</p> <p>A Service Provider shall not, except as permitted or required by law, or with the consent of the person to whom the information relates, collect, use, maintain or disclose customer information for undisclosed or unauthorised purposes. (Article 91, Telecoms By-Laws)</p> <p>Confidentiality Service Providers shall take all reasonable steps to ensure the confidentiality of customer communications. (Article 91, Telecoms By-Laws)</p> <p>Security & technical safeguards Service Providers shall ensure that customer information and customer communications are protected by security and technical safeguards that are appropriate to their sensitivity. (Article 92, Telecoms By-Laws)</p> <p>Third parties A Service Provider shall be responsible for any records, which are under the control of its agents, containing customer information and communications. (Article 92, Telecoms By-Laws)</p> <p>Information to be provided The purposes for which customer information is collected by a Service Provider shall be identified at or before collection. (Article 92, Telecoms By-Laws)</p>	

GDPR	Qatar Data Protection Law	Telecoms Law	General Observations
	<p>Data subject rights The controller must demonstrate the Data Subject's consent to Processing their Personal Data. The consent must be clearly presented and easily distinguished from other matters, in an intelligible and easily accessible form. The consent must be able to be withdrawn at any time. (Article 24)</p> <p>The controller must make reasonable efforts to verify parental consent (when the child is under 16, although in some members states may be as young as 13).</p> <p>Choosing a data processor The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of this Regulation and ensure the protection of the rights of the Data Subject.</p> <p>Processing by a processor shall be governed by a contract or other legal act. (Article 28)</p> <p>Notifications In the case of a Personal Data breach, the controller must notify the supervisory authority of the breach. This must be done without due delay and, where feasible, not later than 72 hours after having become aware of it. (Article 33)</p> <p>Record keeping Each controller must maintain a record of its Processing activities. (Article 30)</p>	<p>review and correct the same directly. (Articles 11(4), (6))</p> <p>Notifications Data controllers must set internal rules for effective management of Personal Data and reporting any breach for the procedures of protecting the same. (Article 11(5))</p> <p>The controller shall advise the individual and concerned department about any breach/violation to the aforementioned precautions if such breach is likely to cause serious damages to the Personal Data or privacy of individuals. (Article 14)</p> <p>Self-audit and review Data controllers must carry out comprehensive audits and reviews about the extent of compliance with Personal Data protection. (Article 11(7))</p>	

GDPR		Qatar Data Protection Law	Telecoms Law	General Observations
Data Subject Rights	<p>Appoint a representative The controller must appoint an EU representative in certain situations. (Article 27)</p> <p>Appoint a DPO The controller must appoint a Data Protection Officer (DPO) in certain situations. (Article 37(1))</p>			
	<p>Transparent communication In order to ensure that Personal Data are processed fairly and lawfully, controllers must provide certain minimum information to Data Subjects, regarding the collection and further Processing of their Personal Data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. (Articles 5(1)(a), 12-14)</p> <p>Data subject rights Data controllers have a legal obligation to give effect to the rights of Data Subjects. (Article 12(2))</p> <p>Identifying data subjects Data controllers must not refuse to give effect to the rights of a Data Subject unless the controller cannot identify the Data Subject. The controller must use all reasonable efforts to verify the identity of Data Subjects. Where the controller has reasonable doubts as to the identity of the Data Subject, the controller may request the provision of additional information necessary to confirm the identity of the Data Subject, but is not required to do so. (Article 12(2), (6))</p>	<p>General principles Every individual has the right in protecting the privacy of his Personal Data, and the same may not be processed except with transparency, integrity and respect for human dignity and acceptable practices. (Article 3)</p> <p>Consent An individual may at any time withdraw his prior consent regarding Processing his Personal Data. (Article 5(1))</p> <p>Object to processing An individual may at any time raise an objection regarding the Processing of his Personal Data if the same was unnecessary for the purposes for which such data were collected, or if the same were extra, discriminative, prejudicing or contradicting the law. (Article 5(2))</p> <p>Erasure An individual may at any time request deletion of his Personal Data pursuant to the aforementioned two clauses or upon achieving the purpose for which such data were collected, or when there is no justification for keeping such data by the Controller. (Article 5(3))</p>	<p>Rectification Customers shall have the right to require that any of their information be corrected. (Article 52)</p> <p>Erasure Customers shall have the right to require that any of their information be removed. (Article 52)</p>	<p>The Qatar Data Protection Law is in the most part influenced by the 1995 Directive. Therefore it is broadly aligned with the GDPR.</p>

GDPR	Qatar Data Protection Law	Telecoms Law	General Observations
	<p>Time limits A controller must, within one month of receiving a request made under those rights, provide any requested information in relation to any of the rights of Data Subjects. If the controller fails to meet this deadline, the Data Subject may complain to the relevant DPSA and may seek a judicial remedy. Where a controller receives large numbers of requests, or especially complex requests, the time limit may be extended by a maximum of two further months. (Article 12(3) - (4))</p> <p>Basic information Data Subjects have the right to be provided with information on the identity of the controller, the reasons for Processing their Personal Data and other relevant information necessary to ensure the fair and transparent Processing of Personal Data. (Articles 13 and 14)</p> <p>Right of access Data Subjects have the right to obtain the following:</p> <ul style="list-style-type: none"> • confirmation of whether, and where, the controller is Processing their Personal Data; • information about the purposes of the Processing; • information about the categories of data being processed; • information about the categories of recipients with whom the data may be shared; • information about the period for which the data will be stored (or the criteria used to determine that period); 	<p>Rectification An individual may at any time submit a request for correcting his Personal Data, appended with supporting documents. (Article 5(4))</p> <p>Right of access An individual may, at any time, get access to his Personal Data or request any controller to review them; in particular he is entitled:</p> <ul style="list-style-type: none"> • to be advised about the Processing of his Personal Data and the purposes of such Processing. • to be advised when any inaccurate Personal Data were disclosed about him. • to obtain a copy of his Personal Data after paying charges not exceeding the value of the service. (Article 6) <p>Information to be provided The controller shall, before Processing any Personal Data, tell the individual about the following:</p> <ul style="list-style-type: none"> • Details of the controller or any other party assuming the task of Processing data for the controller or for its own use. • The legal purposes for which the controller or any other party wish to process Personal Data. • The full and accurate description of the Processing activities and levels of disclosing Personal Data for legal purposes, or if the controller was not able to do that, he shall enable the individual to have a general description about the same. 	

GDPR	Qatar Data Protection Law	Telecoms Law	General Observations
	<ul style="list-style-type: none"> information about the existence of the rights to erasure, to rectification, to restriction of Processing and to object to Processing; information about the existence of the right to complain to the DPSC; where the data were not collected from the Data Subject, information as to the source of the data; and information about the existence of, and an explanation of the logic involved in any automated Processing that has a significant effect on Data Subjects; and Data Subjects may request a copy of the Personal Data being processed. (Article 15) <p>Access fees Data controllers must give effect to the rights of access, rectification, erasure and the right to object, free of charge. The controller may charge a reasonable fee for "repetitive requests", "manifestly unfounded or excessive requests" or "further copies". (Articles 12(5), 15(3), (4))</p> <p>Rectification Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data Subjects have the right to rectification of inaccurate Personal Data. (Articles 5(1)(d), 16)</p> <p>Erasure Data Subjects have the right to erasure of Personal Data if:</p> <ul style="list-style-type: none"> the data are no longer needed for their original purpose (and no new lawful purpose exists); 	<ul style="list-style-type: none"> Any other necessary information for meeting the conditions of Processing Personal Data. (Article 9) <p>Right to information The controller shall advise the individual and concerned department about any breach/violation to the aforementioned precautions if such breach is likely to cause serious damages to the Personal Data or privacy of individuals. (Article 14)</p> <p>Direct marketing An individual may not be subject to any direct electronic marketing communication without their prior consent. The electronic communication should:</p> <ul style="list-style-type: none"> demonstrate the identity of the marketer and proof for direct marketing purposes include an address via which the marketer can be contacted by the individual including to send a request for the purpose of stopping such communications or withdrawing consent to the same. (Article 22) <p>Exemptions Data controllers are be exempted from disclosing the reasons of refusing to comply with the rights of the individual under Article 6 if:</p> <ul style="list-style-type: none"> such disclosure may prevent achieving the purposes stipulated in Article 18. (Article 20) the disclosure will prejudice the commercial interests of another person; (Article 21(1)) the implementation of such obligation leads to disclosing personal details of another person who did not agree on the 	

GDPR	Qatar Data Protection Law	Telecoms Law	General Observations
	<ul style="list-style-type: none"> the lawful basis for the Processing is the Data Subject's consent, the Data Subject withdraws that consent, and no other lawful ground exists; the Data Subject exercises the right to object, and the controller has no overriding grounds for continuing the Processing; the data have been processed unlawfully; or erasure is necessary for compliance with EU law or the national law of the relevant Member State. (Article 17) <p>Restrict processing Data Subjects have the right to restrict the Processing of Personal Data (meaning that the data may only be held by the controller, and may only be used for limited purposes) if:</p> <ul style="list-style-type: none"> the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); the Processing is unlawful and the Data Subject requests restriction (as opposed to exercising the right to erasure); the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or if verification of overriding grounds is pending, in the context of an erasure request. (Article 18) 	<p>same, or if the disclosure may cause material or immaterial damages to such individual or any other individual. (Article 21(2))</p>	

GDPR	Qatar Data Protection Law	Telecoms Law	General Observations
<p>Portability Data Subjects have a right to:</p> <ul style="list-style-type: none"> • receive a copy of their Personal Data in a structured, commonly used, machine-readable format that supports re-use; • transfer their Personal Data from one controller to another; • store their Personal Data for further personal use on a private device; and • have their Personal Data transmitted directly between controllers without hindrance. (Article 20) <p>Object to processing Data Subjects have the right to object, on grounds relating to their particular situation, to the Processing of Personal Data, where the basis for that Processing is either:</p> <ul style="list-style-type: none"> • public interest; or • legitimate interests of the controller. <p>The controller must cease such Processing unless the controller:</p> <ul style="list-style-type: none"> • demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject; or • requires the data in order to establish, exercise or defend legal rights. (Article 21) <p>Where Personal Data are processed for scientific and historical research purposes or statistical purposes, the Data Subject has the right to object, unless the Processing is necessary for the</p>			

GDPR	Qatar Data Protection Law	Telecoms Law	General Observations
<p>performance of a task carried out for reasons of public interest. (Articles 21(6), 83(1))</p> <p>Object to direct marketing Data Subjects have the right to object to the Processing of Personal Data for the purpose of direct marketing, including profiling. (Article 21(2) – (3))</p> <p>Duty to inform of right to object The right to object to Processing of Personal Data noted above must be communicated to the Data Subject no later than the time of the first communication with the Data Subject.</p> <p>This information should be provided clearly and separately from any other information provided to the Data Subject. (Articles 3(2)(b), 14(2)(c), 15(1)(e), 21(4))</p> <p>Automated processing Data Subjects have the right not to be subject to a decision based solely on automated Processing which significantly affect them (including profiling). Such Processing is permitted where:</p> <ul style="list-style-type: none"> • it is necessary for entering into or performing a contract with the Data Subject provided that appropriate safeguards are in place; • it is authorised by law; or • the Data Subject has explicitly consented and appropriate safeguards are in place. (Article 22) 			

	GDPR	Qatar Data Protection Law	Telecoms Law	General Observations
Cross-Border Transfer Rules	<p>General prohibition Cross-Border Personal Data Transfers may only take place if the transfer is made to an Adequate Jurisdiction or the data exporter has implemented a lawful data transfer mechanism (or an exemption or derogation applies). (Articles 44, 45)</p> <p>Adequacy decisions Cross-border data transfers may take place if the third country receives an Adequacy Decision from the EU Commission. (Articles 44, 45)</p> <p>The EU Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the USA (subject to compliance with the terms of the US-EU Privacy Shield).</p> <p>Public authorities Cross-border data transfers between public authorities may take place under agreements between public authorities, which do not require any specific authorisation from a DPSA. (Articles 46(2)(a), 46(3)(b))</p> <p>Binding Corporate Rules Cross-Border Transfer within a corporate group may take place on the basis of Binding Corporate Rules ("BCRs"). BCRs require approval from DPSAs, but approved, individual transfers made under the BCRs do not require further approval. (Articles 4(20) 46(2)(b), 47)</p> <p>Model clauses Cross-border data transfers may take place on the basis of the Model Clauses</p>	<p>General prohibition Data controllers may not process (i.e. transfer) Personal Data of Data Subjects without their consent unless the Processing is deemed necessary for realising a 'lawful purpose' for the controller or for the third party to whom the Personal Data is sent. (Articles 3, 4, 12)</p> <p>Derogations A Trans-border Data Flow may occur where the data exporter is:</p> <ul style="list-style-type: none"> performing a task pertaining to the public good; executing a court order; protecting the vital interests of the individual; meeting the objectives of scientific research; collecting information to investigate a crime when asked by officials. (Article 19) <p>Note: 'Trans-border Data Flow' means accessing, viewing, retrieving, using or storing Personal Data without the constraints of state borders.</p> <p>Restricting data flows Data controllers should not take measures or adopt procedures that may limit Trans-border Data Flows, unless Processing such data violates the provisions of the Qatar Data Protection Law or will cause gross damage to the Data Subject. (Article 15)</p>	<p>No specific provisions exist.</p> <p>Telecoms by-laws</p> <p>General prohibition A Service Provider shall not disclose customer information to any person without the customer's consent, unless disclosure is required or permitted by the General Secretariat in accordance with the applicable laws or regulations of the State of Qatar. (Article 92, Telecoms By-Laws)</p>	<p>The rules surrounding cross-border data transfers in the Qatar Data Protection Law, being based on the 1995 Directive, mirror to a significant extent those in the GDPR. The GDPR however, whilst maintaining the existing data transfer mechanisms created under the 1995 Directive (with some minor amendments), also creates a number of new transfer mechanisms.</p> <p>NOTE: Under the GDPR, cross-border data transfers may take place on the basis of standard data protection clauses approved by the EU Commission ("Model Clauses"). The current set of Model Clauses are currently being challenged as a form of appropriate data transfer mechanism; therefore their future is uncertain.</p> <p>In January 2019, the Irish Supreme Court (as part of the <i>Schrems v Facebook</i> litigation) heard an appeal by Facebook over a decision of the Irish High Court to refer a number of questions to the Court of Justice of the EU ("CJEU") regarding the validity of this data transfer mechanism. The Supreme Court will publish its decision in due course. If Facebook is unsuccessful in its appeal, the CJEU will rule on these questions, which may result in a declaration that the Model Clauses are no longer valid as a transfer mechanism.</p>

GDPR	Qatar Data Protection Law	Telecoms Law	General Observations
	<p>entered into between the data exporter and data recipient. Existing Model Clauses implemented under the 1995 Directive remain valid until amended, replaced or repealed under the GDPR. (Articles 28(6)-(8), 46(2)(c), 57(1)(j), (r), 93(2))</p> <p>Other mechanisms Cross-border data transfers may take place on the basis, <i>inter alia</i>, of:</p> <ul style="list-style-type: none"> • standard data protection clauses adopted by one or more DPSAs under the GDPR. (Articles 46(2)(d), 64(1)(d), 57(1)(j), (r), 93(2)) • an approved code of conduct, together with binding and enforceable commitments to provide appropriate safeguards. (Articles 40, 41, 46(2)(e)) • certifications together with binding and enforceable commitments of the data importer to apply the certification to the transferred data. (Articles 42, 43, 46(2)(f)) • ad hoc clauses conforming to the GDPR and approved by the relevant DPSA. (Articles 46(3)(a), (4), 63)) • administrative arrangements between public authorities (e.g., MOUs) subject to DPSA approval. (Articles 46(3)(b), (4), 63) <p>Derogations Cross-border data transfers may be made on the basis, <i>inter alia</i>, that:</p> <ul style="list-style-type: none"> • the Data Subject explicitly consents having been informed of the possible risks of such transfer. (Article 49(1)(a), (3)) • the performance of a contract between the Data Subject and the controller. (Article 49(1)(b), (3)) 		

GDPR		Qatar Data Protection Law	Telecoms Law	General Observations
	<ul style="list-style-type: none"> it is necessary for the purposes of performing or concluding a contract in the interests of the Data Subject. (Article 49(1)(c), (3)) the transfer is necessary for important reasons of public interest. (Article 49(1)(d), (4)) it is necessary for the purposes of legal proceedings, or obtaining legal advice. (Article 49(1)(e)) the transfer is necessary in order to protect the vital interests of the Data Subject, where the Data Subject is incapable of giving consent. (Article 49(1)(f)) the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by those of the individual subject to informing the relevant DPSA and the Data Subjects. (Article 49(1), (3), (6)) 			
Personal Data Security	<p>Security Data controllers must implement appropriate technical and organisational security measures to protect Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.</p> <p>Depending on the nature of the Processing, these measures may include:</p> <ul style="list-style-type: none"> encryption of the Personal Data; on-going reviews of security measures; redundancy and back-up facilities; and regular security testing. (Article 32) 	<p>Security The controller shall take the appropriate administrative, technical and material precautions to protect Personal Data as determined by the concerned department. (Article 8(3))</p> <p>Both the controller and processor shall take the required precautions to protect Personal Data from loss, damage, amendment, disclosure, access or use incidentally or illegally. Such precautions shall be suitable for the nature and importance of the Personal Data to be protected. The processor shall advise the controller about any breach/violation to such precautions or any risk to the Personal Data of individuals, whatsoever,</p>	<p>No specific provisions exist.</p> <p>Telecoms by-laws</p> <p>Security & technical safeguards Service Providers shall ensure that customer information and customer communications are protected by security and technical safeguards that are appropriate to their sensitivity. (Article 92)</p>	<p>Being based on the 1995 Directive, the Qatar Data Protection Law leaves a significant amount of discretion to the controller in terms of the technical and organisational measures to be implemented in the controller's particular context. The GDPR is more prescriptive but the net effect is very similar.</p>

GDPR		Qatar Data Protection Law	Telecoms Law	General Observations
		as soon as he knows about the same. (Article 13)		
Administrative Fines and Regulatory Sanctions	Judicial remedies Data Subjects have the right to an effective judicial remedy against: <ul style="list-style-type: none"> • decisions of a DPSA concerning them; • any failure by a DPSA to deal with, or respond to, a complaint within three months; and • any unlawful Processing of their Personal Data by a controller or processor. (Article 78-79) 	Administrative fines Violations of the law may attract the following penalties: <ul style="list-style-type: none"> • breach of Articles 4, 8, 9, 10, 11, 12, 14, 15, and 22 – fine not exceeding 1,000,000 Riyals; (Article 23) • breach of Articles 13, 16(3) and 17 – fine not exceeding 5,000,000 Riyals; (Article 24) and • 1,000,000 Riyals for any breach by a body corporate. (Article 25) 	Obtaining data Any person who deliberately accesses a telecommunications facility, network or a system attached thereto by penetrating security measures for the purposes of obtaining data shall be subject to: <ul style="list-style-type: none"> • imprisonment for not more than 1 year: and/or • a fine up to 50,000 Riyals. (Article 66) 	The GDPR carries significantly more severe penalties than the Qatar Data Protection Law or Telecoms Law.
	Compensation & liability A Data Subject who has suffered harm as a result of the unlawful Processing of his or her Personal Data has the right to receive compensation from the controller or processor for the harm suffered: <ul style="list-style-type: none"> • Any controller involved in the Processing is liable for the harm caused. • A processor is liable for the harm caused by any of its (or its sub-processor's) Processing activities that are not in compliance with its obligations under the GDPR, or are in breach of the controller's instructions. • To ensure effective compensation, each controller or processor will be held liable for the entirety of the harm caused, if they are involved in the same Processing and responsible for that harm. (Article 82(1)-(2), (4)) 		Divulging information Any person who, in the course of their employment in the telecommunications field or as a result thereof: <ul style="list-style-type: none"> • divulges, spreads, publishes or records all or part of the content of a telecommunications message, without legal authority; • hides, alters, obstructs or changes all or part of any telecommunications message that reached the person; • divulges of any information concerning users of telecommunications networks or of their communications that are made or received, without legal authority, shall be subject to: <ul style="list-style-type: none"> • imprisonment for not more than 1 year: and/or • a fine up to 100,000 Riyals. (Article 69) 	
	Joint-controller liability Data Subjects are entitled to enforce their rights against any of the joint controllers.		Management liability The person responsible for the actual management of the corporate person shall	

GDPR	Qatar Data Protection Law	Telecoms Law	General Observations
<p>Each joint controller is liable for the entirety of the damage, although national law may apportion liability between them. If one joint controller has paid full compensation, it may then bring proceedings against the other joint controllers to recover their portions of the damages. (Article 26(3), 82(3)-(5))</p> <p>Exemptions from liability A controller or processor is exempt from liability if it proves that it is not responsible for the event giving rise to the harm. There is no mention of force majeure events. (Article 82(3))</p> <p>Administrative fines The maximum fine that can be imposed for serious infringements of the GDPR is the greater of €20 million or 4% of an undertaking's worldwide turnover for the preceding financial year. (Article 83(5) – (6))</p> <p>Fine criteria When deciding whether to impose a fine and deciding on the amount, DPSAs are required to give due regard to a range of issues, including:</p> <ul style="list-style-type: none"> • the nature, gravity and duration of the infringement; • the number of Data Subjects affected and the level of harm suffered by them; • the intentional or negligent character of the infringement; • any action taken by the controller or processor to mitigate the harm; • any relevant previous infringements by the controller or processor; • the degree of co-operation with the relevant DPSA; 		<p>be punished with the same penalties assigned to the acts that are committed in violation of the law if it is proved that such person was aware of such acts or the breach of their duties rendered upon them by such management, had contributed to the offence. (Article 71)</p> <p>Repeat offences All penalties shall be doubled for any person who commits an offence specified herein within three years from the date of the fulfilment of a previous penalty. (Article 72)</p>	

GDPR		Qatar Data Protection Law	Telecoms Law	General Observations
	<ul style="list-style-type: none"> whether the infringement was self-reported by the controller or processor; and any other aggravating or mitigating factors. (Article 82(3)) 			
Role and Powers of any relevant Data Protection Supervisory Authority	<p>Independence DPSAs must act independently and operate free from all outside influences, including government control. (Article 52)</p> <p>Tasks The tasks of DPSAs include obligations to:</p> <ul style="list-style-type: none"> monitor and enforce the application of the GDPR; promote awareness of the risks, rules, safeguards and rights pertaining to Personal Data (especially in relation to children); advise national and governmental institutions on the application of the GDPR; hear claims brought by Data Subjects or their representatives, and inform Data Subjects of the outcome of such claims; establish requirements for Impact Assessments; encourage the creation of Codes of Conduct and review certifications; authorise Model Clauses and BCRs; keep records of sanctions and enforcement actions; and fulfil "any other tasks related to protection of Personal Data". (Article 55, 57) 	<p>Investigations On foot of a complaint filed by an individual, the Qatar Ministry of Transport and Communications (MOTC) may, after investigating the complaint and verifying the same, issue a justified order binding the controller or processor, as the case may be, to rectify such violation within a fixed period. The controller or processor may file a grievance against such order to the Minister within sixty days from the date of notification. The resolution of the Minister regarding such grievance shall be deemed final. (Article 26)</p> <p>Seizure Judicial officers/law enforcement officers designated by the MOTC have the power to seize and document any crimes related to violating the provisions of the law. (Article 29)</p>	<p>Search, investigate and seize In respect of any suspected offence under the law, the regulator may enter premises, have access to records and documents and inspect equipment and telecommunications systems or any other related things and request data or clarifications as they deem necessary. (Article 63)</p>	Under the GDPR, DPSAs are considered to have more significant supervisory and enforcement powers when compared with Qatar.

GDPR		Qatar Data Protection Law	Telecoms Law	General Observations
	<p>Powers DPSAs are empowered to oversee enforcement of the GDPR, investigate breaches of the GDPR and bring legal proceedings where necessary. (Article 58)</p>			

QATAR FINANCIAL CENTRE



Qatar Financial Centre – Executive summary

This jurisdictional overview is based on an unofficial English translation of the Law No 13 of 2016 Concerning Personal Data Protection. The Qatar government does not issue official English translations of the laws of the State of Qatar.

The Qatar Financial Centre ("**QFC**") introduced its own Data Protection Regulations No 6 of 2005 and Data Protection Rules 2005 (the "**QFC Data Protection Laws**"). In addition, the State of Qatar was the first GCC nation to issue a generally applicable data protection law when it implemented Law No 13 of 2016 Concerning Personal Data Protection (the "**Qatar Data Protection Law**"). As the Qatar Data Protection Law does not expressly exclude the QFC from its provisions, it would be prudent to assume that QFC-registered businesses are also subject to its requirements.

The Data Protection Directorate (**DPD**) is responsible for implementing and enforcing the QFC Data Protection Laws, managing related disputes and applying GDPR standards. The DPD is led by a Data Protection Officer certified by the European Centre for Privacy and Cybersecurity from

Maastricht University. The law applies in the jurisdiction of the QFC and is therefore applicable to all QFC entities, both regulated and non-regulated by the QFC Regulatory Authority.

The QFC Data Protection Laws are largely modelled on, and inspired by, the privacy and data protection principles and guidelines contained in the 1995 Directive and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

The concepts and requirements of the DPL will be clarified in further ministerial decisions and interviews with the QFC Employment Standards Office indicate that the next step for the QFC will be the full alignment of the QFC Data Protection Laws with the GDPR.

	GDPR	QFC Data Protection Laws	General Observations
Principles of Data Processing	<p>Lawfulness, fairness, transparency Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. (Article 5(1)(a))</p> <p>Specified purposes Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. (Article 5(1)(b))</p> <p>Data minimisation Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. (Article 5(1)(c))</p> <p>Accuracy Personal Data must be accurate and, where necessary, kept up to date. (Article 5(1)(d))</p> <p>Storage limitation Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. (Article 5(1)(e))</p> <p>Integrity and confidentiality Personal Data must be processed in a way 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. (Article 5(1)(f))</p> <p>Accountability The controller shall be responsible for and be able to demonstrate compliance with all the above principles. (Article 5(2))</p>	<p>Lawful processing Data Controllers must ensure that Personal Data which they process is processed fairly, lawfully and securely. (Article 6(1)(A))</p> <p>Specified purposes Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. (Article 6(1)(B))</p> <p>Data minimisation Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. (Article 6(1)(C))</p> <p>Accuracy Personal Data must be accurate and, where necessary, kept up to date. (Article 6(1)(D))</p> <p>Storage limitation Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. (Article 6(1)(E))</p> <p>Inaccuracies Every reasonable step must be taken by Data Controllers to ensure that Personal Data which is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further processed, is erased or rectified. (Article 6(2))</p> <p>Lawful bases Data controllers may process Personal Data when any of the following conditions are met:</p> <ul style="list-style-type: none"> the Data Subject has given their unambiguous consent to the Processing (Article 7(1)) 	<p>The QFC Data Protection Laws are in the most part influenced by the 1995 Directive. Therefore they are broadly aligned with the GDPR.</p>

GDPR		QFC Data Protection Laws	General Observations
Data Controller and Data Processor Obligations	<p>Lawful bases The legal bases under which Personal Data may be processed are:</p> <ul style="list-style-type: none"> with the freely given, specific, informed and unambiguous consent of the Data Subject; where necessary for the performance of a contract to which the Data Subject is party; where necessary to comply with a legal obligation to which the controller is subject; where necessary to protect the vital interests of the Data Subject or another person; where 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 where necessary for the purposes of the legitimate interests of the controller or a third party. (Article 6(1)) 	<ul style="list-style-type: none"> the Processing is necessary for the performance of a contract to which the Data Subject is party (Article 7(2)) the Processing is necessary for compliance with any legal obligation to which the data controller is subject (Article 7(3)) the Processing is necessary in order to protect the vital interests of the Data Subject (Article 7(4)) the Processing is necessary for the performance of public tasks carried out in the interests of the QFC, or in the exercise of the QFC Authority, the QFC Regulatory Authority, the QFC Tribunal or Appeals Body functions or powers vested in the data controller or in a third party to whom the Personal Data is disclosed (Article 7(5)) the 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 (Article 7(6)) 	
	<p>General principles The controller is responsible for compliance with the principles listed in Article 5 (as set out above).</p> <p>The controller must have regard to 'data protection by design and by default' throughout their Processing activities.</p> <p>Lawful processing The controller must carry only process Personal Data under one of the conditions laid out in Article 6 and for special categories of Personal Data those laid out in Article 9.</p> <p>Sensitive personal data The Processing of sensitive Personal Data is prohibited, unless the:</p> <ul style="list-style-type: none"> Data Subject has given explicit consent. (Article 9(2)(a)) 	<p>Lawful processing The controller must only process Personal Data under one of the conditions laid out in Article 7 and for special categories of Personal Data those laid out in Article 8.</p> <p>Technical & organisational measures The Data Controller must implement appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of Processing, in particular where Processing sensitive Personal Data or transferring Personal Data to another jurisdiction. (Article 14(1))</p> <p>Confidentiality Any person acting under a Data Controller or a Data Processor, including the Data Processor himself, who has access to Personal Data, must not process it except on instructions from the Data Controller, unless he is required to do so by law. (Article 13)</p>	The QFC, being based on the 1995 Directive, largely mirrors the GDPR in terms of obligations imposed on Data Controllers and Data Processors

GDPR	QFC Data Protection Laws	General Observations
	<ul style="list-style-type: none"> Processing is necessary in the context of employment law, or laws relating to social security and social protection. (Article 9(2)(b)) Processing is necessary to protect vital interests of the Data Subject (or another person). (Article 9(2)(c)) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim. (Article 9(2)(d)) Processing relates to Personal Data which are manifestly made public by the Data Subject. (Article 9(2)(e)) Processing is necessary for the establishment, exercise or defence of legal claims. (Article 9(2)(f)) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law. (Article 9(2)(g)) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional. (Article 9(2)(h)) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law. (Article 9(2)(i)) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. (Article 9(2)(j)) <p>Record keeping Each Data Controller must establish and maintain a record of all wholly or partly automatic Personal Data Processing operations or set of such operations intended to secure a single purpose or several related purposes. (Article 17(1))</p> <p>Notifications There is no requirement under the QFC Data Protection Laws to inform the QFC Authority of any breaches of Personal Data databases.</p>	

GDPR	QFC Data Protection Laws	General Observations
<p>Technical & organisational measures The controller is responsible for implementing appropriate technical and organisational measures to ensure and demonstrate that its Processing activities are compliant with the requirements of the GDPR. (Article 32)</p> <p>Data subject rights The controller must demonstrate the Data Subject's consent to Processing their Personal Data. The consent must be clearly presented and easily distinguished from other matters, in an intelligible and easily accessible form. The consent must be able to be withdrawn at any time. (Article 24)</p> <p>The controller must make reasonable efforts to verify parental consent (when the child is under 16, although in some members states may be as young as 13).</p> <p>Choosing a data processor The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of this Regulation and ensure the protection of the rights of the Data Subject.</p> <p>Processing by a processor shall be governed by a contract or other legal act. (Article 28)</p> <p>Notifications In the case of a Personal Data breach, the controller must notify the supervisory authority of the breach. This must be done without due delay and, where feasible, not later than 72 hours after having become aware of it. (Article 33)</p> <p>Record keeping Each controller must maintain a record of its Processing activities. (Article 30)</p>		

GDPR		QFC Data Protection Laws	General Observations
	<p>Appoint a representative The controller must appoint an EU representative in certain situations. (Article 27)</p> <p>Appoint a DPO The controller must appoint a Data Protection Officer (DPO) in certain situations. (Article 37(1))</p>		
Data Subject Rights	<p>Transparent communication In order to ensure that Personal Data are processed fairly and lawfully, controllers must provide certain minimum information to Data Subjects, regarding the collection and further Processing of their Personal Data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. (Articles 5(1)(a), 12-14)</p> <p>Data Subject rights Data controllers have a legal obligation to give effect to the rights of Data Subjects. (Article 12(2))</p> <p>Identifying data subjects Data controllers must not refuse to give effect to the rights of a Data Subject unless the controller cannot identify the Data Subject. The controller must use all reasonable efforts to verify the identity of Data Subjects. Where the controller has reasonable doubts as to the identity of the Data Subject, the controller may request the provision of additional information necessary to confirm the identity of the Data Subject, but is not required to do so. (Article 12(2), (6))</p> <p>Time limits A controller must, within one month of receiving a request made under those rights, provide any requested information in relation to any of the rights of Data Subjects. If the controller fails to meet this deadline, the Data Subject may complain to the relevant DPSA and may seek a judicial remedy. Where a controller receives large numbers of requests, or especially complex requests, the time limit may be</p>	<p>Basic information Data Subjects have the right to be provided with information on the identity of the controller, the reasons for Processing their Personal Data and other relevant information necessary to ensure the fair and transparent Processing of Personal Data including:</p> <ul style="list-style-type: none"> • parties with whom the Personal Data may be shared; • the Personal Data/ categories of Personal Data processed; • whether replies to questions are obligatory or voluntary, as well as the possible consequences of failure to reply; • the existence of the right of access to and the right to rectify the Personal Data; and • whether the Personal Data will be used for direct marketing purposes. (Articles 11 and 12) <p>Right of access A Data Subject has the right to require and obtain from the Data Controller upon request, at reasonable intervals and without excessive delay or expense, confirmation as to whether Personal Data relating to him is being processed and, if so information as to:</p> <ul style="list-style-type: none"> • the purposes of the Processing; • the categories of Personal Data concerned and • the recipients or categories of recipients to whom the Personal Data is disclosed. (Article 15(1)) 	<p>The QFC Data Protection Laws are in the most part influenced by the 1995 Directive. Therefore they are broadly aligned with the GDPR.</p>

GDPR	QFC Data Protection Laws	General Observations
	<p>extended by a maximum of two further months. (Article 12(3) - (4))</p> <p>Basic information Data Subjects have the right to be provided with information on the identity of the controller, the reasons for Processing their Personal Data and other relevant information necessary to ensure the fair and transparent Processing of Personal Data. (Articles 13 and 14)</p> <p>Right of access Data Subjects have the right to obtain the following:</p> <ul style="list-style-type: none"> • confirmation of whether, and where, the controller is Processing their Personal Data; • information about the purposes of the Processing; • information about the categories of data being processed; • information about the categories of recipients with whom the data may be shared; • information about the period for which the data will be stored (or the criteria used to determine that period); • information about the existence of the rights to erasure, to rectification, to restriction of Processing and to object to Processing; • information about the existence of the right to complain to the DPSA; • where the data were not collected from the Data Subject, information as to the source of the data; and • information about the existence of, and an explanation of the logic involved in any automated Processing that has a significant effect on Data Subjects; and • Data Subjects may request a copy of the Personal Data being processed. (Article 15) <p>Transparent communication A Data Subject has the right to require and obtain from the Data Controller upon request, at reasonable intervals and without excessive delay or expense, communication to him in an intelligible form of the Personal Data undergoing Processing and of any available information as to its source. (Article 15(2))</p> <p>Rectification, erasure, blocking A Data Subject has the right to require and obtain from the Data Controller upon request, at reasonable intervals and without excessive delay or expense, as appropriate, the rectification, erasure or blocking of Personal Data the Processing of which does not comply with the law. (Article 15(3))</p> <p>Object to processing A Data Subject has the right to:</p> <ul style="list-style-type: none"> • object at any time on reasonable grounds relating to his particular situation to the Processing of Personal Data relating to him; and • 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. (Article 16(1). (2)) 	

GDPR	QFC Data Protection Laws	General Observations
<p>Access fees Data controllers must give effect to the rights of access, rectification, erasure and the right to object, free of charge. The controller may charge a reasonable fee for "repetitive requests", "manifestly unfounded or excessive requests" or "further copies". (Articles 12(5), 15(3), (4))</p> <p>Rectification Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data Subjects have the right to rectification of inaccurate Personal Data. (Articles 5(1)(d), 16)</p> <p>Erasure Data Subjects have the right to erasure of Personal Data if:</p> <ul style="list-style-type: none"> • the data are no longer needed for their original purpose (and no new lawful purpose exists); • the lawful basis for the Processing is the Data Subject's consent, the Data Subject withdraws that consent, and no other lawful ground exists; • the Data Subject exercises the right to object, and the controller has no overriding grounds for continuing the Processing; • the data have been processed unlawfully; or • erasure is necessary for compliance with EU law or the national law of the relevant Member State. (Article 17) <p>Restrict processing Data Subjects have the right to restrict the Processing of Personal Data (meaning that the data may only be held by the controller, and may only be used for limited purposes) if:</p> <ul style="list-style-type: none"> • the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); 		

GDPR	QFC Data Protection Laws	General Observations
<ul style="list-style-type: none"> the Processing is unlawful and the Data Subject requests restriction (as opposed to exercising the right to erasure); the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or if verification of overriding grounds is pending, in the context of an erasure request. (Article 18) <p>Portability Data Subjects have a right to:</p> <ul style="list-style-type: none"> receive a copy of their Personal Data in a structured, commonly used, machine-readable format that supports re-use; transfer their Personal Data from one controller to another; store their Personal Data for further personal use on a private device; and have their Personal Data transmitted directly between controllers without hindrance. (Article 20) <p>Object to processing Data Subjects have the right to object, on grounds relating to their particular situation, to the Processing of Personal Data, where the basis for that Processing is either:</p> <ul style="list-style-type: none"> public interest; or legitimate interests of the controller. <p>The controller must cease such Processing unless the controller:</p> <ul style="list-style-type: none"> demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject; or requires the data in order to establish, exercise or defend legal rights. (Article 21) 		

GDPR	QFC Data Protection Laws	General Observations
	<p>Where Personal Data are processed for scientific and historical research purposes or statistical purposes, the Data Subject has the right to object, unless the Processing is necessary for the performance of a task carried out for reasons of public interest. (Articles 21(6), 83(1))</p> <p>Object to direct marketing Data Subjects have the right to object to the Processing of Personal Data for the purpose of direct marketing, including profiling. (Article 21(2) – (3))</p> <p>Duty to inform of right to object The right to object to Processing of Personal Data noted above must be communicated to the Data Subject no later than the time of the first communication with the Data Subject.</p> <p>This information should be provided clearly and separately from any other information provided to the Data Subject. (Articles 3(2)(b), 14(2)(c), 15(1)(e), 21(4))</p> <p>Automated processing Data Subjects have the right not to be subject to a decision based solely on automated Processing which significantly affect them (including profiling). Such Processing is permitted where:</p> <ul style="list-style-type: none"> • it is necessary for entering into or performing a contract with the Data Subject provided that appropriate safeguards are in place; • it is authorised by law; or • the Data Subject has explicitly consented and appropriate safeguards are in place. (Article 22) 	
<p>Cross-Border Transfer Rules</p>	<p>General prohibition Cross-Border Personal Data Transfers may only take place if the transfer is made to an Adequate Jurisdiction or the data exporter has implemented a lawful data transfer mechanism (or an exemption or derogation applies). (Articles 44, 45)</p>	<p>General prohibition Cross-border data transfers may only take place if the transfer is made to an Adequate Jurisdiction that ensures an adequate level of protection for the Personal Data. (Article 9(1))</p> <p>The rules surrounding cross-border data transfers in the QFC, being based on the 1995 Directive, mirror to a significant extent those in the GDPR. The GDPR however, whilst maintaining the existing data transfer mechanisms created under the 1995 Directive (with</p>

GDPR	QFC Data Protection Laws	General Observations
	<p>Adequacy decisions Cross-border data transfers may take place if the third country receives an Adequacy Decision from the EU Commission. (Articles 44, 45)</p> <p>The EU Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the USA (subject to compliance with the terms of the US-EU Privacy Shield).</p> <p>Public authorities Cross-border data transfers between public authorities may take place under agreements between public authorities, which do not require any specific authorisation from a DPSA. (Articles 46(2)(a), 46(3)(b))</p> <p>Binding Corporate Rules Cross-Border Data Transfer within a corporate group may take place on the basis of Binding Corporate Rules ("BCRs"). BCRs require approval from DPSAs, but approved, individual transfers made under the BCRs do not require further approval. (Articles 4(20) 46(2)(b), 47)</p> <p>Model clauses Cross-border data transfers may take place on the basis of the Model Clauses entered into between the data exporter and data recipient. Existing Model Clauses implemented under the 1995 Directive remain valid until amended, replaced or repealed under the GDPR. (Articles 28(6)-(8), 46(2)(c), 57(1)(j), (r), 93(2))</p> <p>Other mechanisms Cross-border data transfers may take place on the basis, <i>inter alia</i>, of:</p> <ul style="list-style-type: none"> standard data protection clauses adopted by one or more DPSAs under the GDPR. (Articles 46(2)(d), 64(1)(d), 57(1)(j), (r), 93(2)) <p>Adequate jurisdictions The QFC Authority (QFCA) does not maintain a list of "adequate" jurisdictions. Rather, the data controller must determine whether a jurisdiction has adequate protection, taking into account:</p> <ul style="list-style-type: none"> the nature of the data; the purpose and duration of the proposed data Processing operations; and any relevant laws to which the recipient of the data is subject. (Article 9(1)) <p>Derogations A Cross-Border Transfer to a recipient in a country not deemed as providing an adequate level of protection for the Personal Data where, <i>inter alia</i>, the:</p> <ul style="list-style-type: none"> QFC DPSA has granted a permit for the transfer and the data controller applies certain adequate safeguards (Article 10(1)(A)); Data Subject has given their unambiguous consent to the proposed transfer (Article 10(1)(B)); transfer is necessary for the performance of a contract between the Data Subject and the data controller (Article 10(1)(C)); 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 (Article 10(1)(D)); transfer is necessary or legally required on grounds important in the interests of the QFC, or for the establishment, exercise or defense of legal claims (Article 10(1)(E)); transfer is necessary to protect the vital interests of the Data Subject (Article 10(1)(F)); transfer is made from a register intended to provide information to the public and which is open to consultation (Article 10(1)(G)); 	<p>some minor amendments), also creates a number of new transfer mechanisms.</p> <p>NOTE: Under the GDPR, cross-border data transfers may take place on the basis of standard data protection clauses approved by the EU Commission ("Model Clauses"). The current set of Model Clauses are currently being challenged as a form of appropriate data transfer mechanism; therefore their future is uncertain.</p> <p>In January 2019, the Irish Supreme Court (as part of the <i>Schrems v Facebook</i> litigation) heard an appeal by Facebook over a decision of the Irish High Court to refer a number of questions to the Court of Justice of the EU ("CJEU") regarding the validity of this data transfer mechanism. The Supreme Court will publish its decision in due course. If Facebook is unsuccessful in its appeal, the CJEU will rule on these questions, which may result in a declaration that the Model Clauses are no longer valid as a transfer mechanism.</p>

GDPR	QFC Data Protection Laws	General Observations
	<ul style="list-style-type: none"> • an approved code of conduct, together with binding and enforceable commitments to provide appropriate safeguards. (Articles 40, 41, 46(2)(e)) • certifications together with binding and enforceable commitments of the data importer to apply the certification to the transferred data. (Articles 42, 43, 46(2)(f)) • ad hoc clauses conforming to the GDPR and approved by the relevant DPSA. (Articles 46(3)(a), (4), 63)) • administrative arrangements between public authorities (e.g., MOUs) subject DPSA approval. (Articles 46(3)(b), (4), 63) <p>Derogations Cross-border data transfers may be made on the basis, <i>inter alia</i>, that:</p> <ul style="list-style-type: none"> • the Data Subject explicitly consents having been informed of the possible risks of such transfer. (Article 49(1)(a), (3)) • the performance of a contract between the Data Subject and the controller. (Article 49(1)(b), (3)) • it is necessary for the purposes of performing or concluding a contract in the interests of the Data Subject. (Article 49(1)(c), (3)) • the transfer is necessary for important reasons of public interest. (Article 49(1)(d), (4)) • it is necessary for the purposes of legal proceedings, or obtaining legal advice. (Article 49(1)(e)) • the transfer is necessary in order to protect the vital interests of the Data Subject, where the Data Subject is incapable of giving consent. (Article 49(1)(f)) • the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by those of the individual subject to informing the relevant DPSA and the Data Subjects. (Article 49(1), (3), (6)) 	<ul style="list-style-type: none"> • transfer is necessary for compliance with any legal obligation to which the data controller is subject (Article 10(1)(H)); • transfer is necessary to uphold the legitimate interests of the data controller recognised in the international financial markets (Article 10(1)(I)); • transfer is necessary to comply with auditing, accounting or anti-money laundering obligations that apply to a data controller (Article 10(1)(J)).

GDPR		QFC Data Protection Laws	General Observations
Personal Data Security	<p>Security Data controllers must implement appropriate technical and organisational security measures to protect Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.</p> <p>Depending on the nature of the Processing, these measures may include:</p> <ul style="list-style-type: none"> • encryption of the Personal Data; • on-going reviews of security measures; • redundancy and back-up facilities; and • regular security testing. (Article 32) 	<p>Technical & organisational measures Data controllers must implement appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of Processing, in particular where sensitive Personal Data is being processed or where the Personal Data is being transferred out of the QFC to a jurisdiction without an adequate level of protection. (Article 14(1))</p> <p>Safeguards on transfer When applying for a permit to process sensitive Personal Data, or transfer Personal Data out of the QFC to a jurisdiction without an adequate level of protection, data controllers must include detail regarding the safeguards employed to ensure the security of Personal Data. (Articles 2.1.1(I), 3.2.1(I))</p> <p>Security The measures implemented by a data controller ought to ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected. (Article 14(2))</p>	Being based on the 1995 Directive, the QFC laws leave a significant amount of discretion to the controller in terms of the technical and organisational measures to be implemented in the controller's particular context. The GDPR is more prescriptive but the net effect is very similar.
	<p>Judicial remedies Data Subjects have the right to an effective judicial remedy against:</p> <ul style="list-style-type: none"> • decisions of a DPSA concerning them; • any failure by a DPSA to deal with, or respond to, a complaint within three months; and • any unlawful Processing of their Personal Data by a controller or processor. (Article 78-79) <p>Compensation & liability A Data Subject who has suffered harm as a result of the unlawful Processing of his or her Personal Data has the right to receive compensation from the controller or processor for the harm suffered:</p>	<p>Directions If the QFC Authority is satisfied that a data controller has contravened or is contravening the law, it may issue a direction to the data controller requiring it to do either or both of the following:</p> <ul style="list-style-type: none"> • to do or refrain from doing any act or thing within such time as may be specified in the direction (Article 22(1)(A)) • to refrain from Processing any Personal Data specified in the direction or to refrain from Processing Personal Data for a purpose or in a manner specified in the direction (Article 22(1)(B)) 	The QFC Data Protection Laws currently impose no financial sanctions on organisations for breaches of the law. For this reason, the QFC rules are considered to lack teeth when compared to the GDPR or the Qatar Data Protection Law.
Administrative Fines and Regulatory Sanctions			

GDPR	QFC Data Protection Laws	General Observations
<ul style="list-style-type: none"> Any controller involved in the Processing is liable for the harm caused. A processor is liable for the harm caused by any of its (or its sub-processor's) Processing activities that are not in compliance with its obligations under the GDPR, or are in breach of the controller's instructions. To ensure effective compensation, each controller or processor will be held liable for the entirety of the harm caused, if they are involved in the same Processing and responsible for that harm. (Article 82(1)-(2), (4)) <p>Joint-controller liability Data Subjects are entitled to enforce their rights against any of the joint controllers. Each joint controller is liable for the entirety of the damage, although national law may apportion liability between them. If one joint controller has paid full compensation, it may then bring proceedings against the other joint controllers to recover their portions of the damages. (Article 26(3), 82(3)-(5))</p> <p>Exemptions from liability A controller or processor is exempt from liability if it proves that it is not responsible for the event giving rise to the harm. There is no mention of force majeure events. (Article 82(3))</p> <p>Administrative fines The maximum fine that can be imposed for serious infringements of the GDPR is the greater of €20 million or 4% of an undertaking's worldwide turnover for the preceding financial year. (Article 83(5) – (6))</p> <p>Fine criteria When deciding whether to impose a fine and deciding on the amount, DPSAs are required to give due regard to a range of issues, including:</p> <ul style="list-style-type: none"> the nature, gravity and duration of the infringement; 		

GDPR		QFC Data Protection Laws	General Observations
	<ul style="list-style-type: none"> the number of Data Subjects affected and the level of harm suffered by them; the intentional or negligent character of the infringement; any action taken by the controller or processor to mitigate the harm; any relevant previous infringements by the controller or processor; the degree of co-operation with the relevant DPSC; whether the infringement was self-reported by the controller or processor; and any other aggravating or mitigating factors. (Article 82(3)) 		
Role and Powers of any relevant Data Protection Supervisory Authority	<p>Independence DPSCs must act independently and operate free from all outside influences, including government control. (Article 52)</p> <p>Tasks The tasks of DPSCs include obligations to:</p> <ul style="list-style-type: none"> monitor and enforce the application of the GDPR; promote awareness of the risks, rules, safeguards and rights pertaining to Personal Data (especially in relation to children); advise national and governmental institutions on the application of the GDPR; hear claims brought by Data Subjects or their representatives, and inform Data Subjects of the outcome of such claims; establish requirements for Impact Assessments; encourage the creation of Codes of Conduct and review certifications; authorise Model Clauses and BCRs; keep records of sanctions and enforcement actions; and fulfil "any other tasks related to protection of Personal Data". (Article 55, 57) 	<p>Powers If the QFC Authority is satisfied that a data controller has contravened or is contravening the law, it may issue a direction to the data controller requiring it to do either or both of the following:</p> <ul style="list-style-type: none"> to do or refrain from doing any act or thing within such time as may be specified in the direction (Article 22(1)(A)) to refrain from Processing any Personal Data specified in the direction or to refrain from Processing Personal Data for a purpose or in a manner specified in the direction (Article 22(1)(B)) <p>The powers and functions of the QFC Authority include the powers and functions to:</p> <ul style="list-style-type: none"> access Personal Data processed by Data Controllers or Data Processors (Article 19(2)(A)) collect all the information necessary for the performance of its supervisory duties (Article 19(2)(B)) prescribe forms to be used for any of the purposes of the law (Article 19(2)(C)) issue warnings or admonishments and make recommendations to Data Controllers (Article 19(2)(D)) 	Under the GDPR, DPSCs are considered to have more significant supervisory and enforcement powers when compared with the QFC.

GDPR		QFC Data Protection Laws	General Observations
	Powers DPSAs are empowered to oversee enforcement of the GDPR, investigate breaches of the GDPR and bring legal proceedings where necessary. (Article 58)	<ul style="list-style-type: none"> bring contraventions of these Regulations to the attention of the relevant tribunal (Article 19(2)(E)) 	

TURKEY



Turkey – Executive summary



The main piece of legislation covering data protection in Turkey is the *Data Protection Law* (Law No 6698 of 7 April 2016) (**Data Protection Law**). Although there are differences, the Data Protection Law is heavily modelled on the 1995 Directive with many of the terms and central provisions very closely mirroring their equivalents in the Directive. The purpose of the Data Protection Law is to:

- put standard practices and procedures in place for the handling of Personal Data; and
- protect the privacy of individuals.

Moreover, grounds for Processing under the Data Protection Law are comparable to the GDPR, save that explicit consent is required when sensitive and non-sensitive Personal Data is processed. Although the Data Protection Law is still in its infancy and there are no enforcement actions yet, the Personal Data Protection Board, the national supervisory authority in Turkey, has published the draft versions of the secondary legislation, as well as some booklets providing guidance on the implementation of the law.

To date, the Turkish legislature has also enacted several important regulations to implement various aspects of the Data Protection Law, including:

- *Regulation on the Erasure, Destruction and Anonymising of Personal Data* (No 30224 of 2017)
- *Regulation on the Working Procedures and Principles of Personal Data Protection Board* (No 30242 of 2017)
- *Regulation on the Registry of Data Controllers* (No 30286 of 2017)
- *Regulation on the Organisation of Personal Data Protection Authority* (No 3040 of 20183)

While the Data Protection Law provides the central framework for the general data protection regime in Turkey, there are also certain industry-specific regulatory measures that introduce further requirements. The most prominent examples of such industry-specific measures are those relating to the electronic communication and banking sectors.

With respect to the telecoms sector, the *Electronic Communications Act 2008* is a regulatory framework for electronic communications networks and contains very limited provisions with respect to privacy and data protection.

GDPR		Data Protection Law	General Observations
Principles of Data Processing	<p>Lawfulness, fairness, transparency Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. (Article 5(1)(a))</p> <p>Specified purposes Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. (Article 5(1)(b))</p> <p>Data minimisation Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. (Article 5(1)(c))</p> <p>Accuracy Personal Data must be accurate and, where necessary, kept up to date. (Article 5(1)(d))</p> <p>Storage limitation Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. (Article 5(1)(e))</p> <p>Integrity and confidentiality Personal Data must be processed in a way 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. (Article 5(1)(f))</p> <p>Accountability The controller shall be responsible for and be able to demonstrate compliance with all the above principles. (Article 5(2))</p> <p>Lawful bases The legal bases under which Personal Data may be processed are:</p>	<p>Lawfulness The Processing of Personal Data must be in conformity with the law and in good faith. (Article 4(2)(a))</p> <p>Accuracy Personal Data must be accurate and if necessary, kept up to date. (Article 4(2)(b))</p> <p>Specified purposes Personal Data must be processed for specified, explicit and legitimate purposes. (Article 4(2)(c))</p> <p>Data minimisation Personal Data must be relevant, limited and proportionate to the purposes for which it is processed. (Article 4(2)(d))</p> <p>Storage limitation Personal Data must only be kept for the time designated by relevant legislation or necessitated by the purpose for which data are collected. (Article 4(2)(e))</p>	The Data Protection Law is primarily based on the same principles as are found in the 1995 Directive (and by extension the GDPR).

GDPR		Data Protection Law	General Observations
	<ul style="list-style-type: none"> with the freely given, specific, informed and unambiguous consent of the Data Subject; where necessary for the performance of a contract to which the Data Subject is party; where necessary to comply with a legal obligation to which the controller is subject; where necessary to protect the vital interests of the Data Subject or another person; where 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 where necessary for the purposes of the legitimate interests of the controller or a third party. (Article 6(1)) 		
Data Controller and Data Processor Obligations	<p>General principles The controller is responsible for compliance with the principles listed in Article 5 (as set out above). The controller must have regard to 'data protection by design and by default' throughout their Processing activities.</p> <p>Lawful processing The controller must carry only process Personal Data under one of the conditions laid out in Article 6 and for special categories of Personal Data those laid out in Article 9.</p> <p>Sensitive personal data The Processing of sensitive Personal Data is prohibited, unless the:</p> <ul style="list-style-type: none"> Data Subject has given explicit consent. (Article 9(2)(a)) Processing is necessary in the context of employment law, or laws relating to social security and social protection. (Article 9(2)(b)) Processing is necessary to protect vital interests of the Data Subject (or another person). (Article 9(2)(c)) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit 	<p>General principles The controller must only process Personal Data in compliance with the general principles listed in article 4 (as set out above).</p> <p>Data controller must not disclose or misuse Personal Data contrary to this law. (Article 12(4))</p> <p>Data controller must notify the Data Subject and the Board if Personal Data are acquired by others by unlawful means. (Article 12(5))</p> <p>Lawful processing The controller shall not process Personal Data without obtaining the explicit consent of the Data Subject unless one of the below conditions is met:</p> <ul style="list-style-type: none"> It is expressly permitted by any law; (Article 5(2)(a)) It is necessary to protect life or physical integrity of the Data Subject or another person where the Data Subject is incapable of giving consent; (Article 5(2)(b)) It is necessary to process the Personal Data of parties to a contract, where the Processing is directly related to the execution or performance of the contract; (Article 5(2)(c)) It is necessary for compliance with a legal obligation which the controller is subject to; (Article 5(2)(d)) 	Being based on the 1995 Directive, the Data Protection Law largely mirrors the GDPR in terms of obligations imposed on Data Controllers and Data Processors.

GDPR	Data Protection Law	General Observations
	<p>body with a political, philosophical, religious or trade union aim. (Article 9(2)(d))</p> <ul style="list-style-type: none"> Processing relates to Personal Data which are manifestly made public by the Data Subject. (Article 9(2)(e)) Processing is necessary for the establishment, exercise or defence of legal claims. (Article 9(2)(f)) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law. (Article 9(2)(g)) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional. (Article 9(2)(h)) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law. (Article 9(2)(i)) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. (Article 9(2)(j)) <p>Technical & organisational measures The controller is responsible for implementing appropriate technical and organisational measures to ensure and demonstrate that its Processing activities are compliant with the requirements of the GDPR. (Article 32)</p> <p>Data subject rights The controller must demonstrate the Data Subject's consent to Processing their Personal Data. The consent must be clearly presented and easily distinguished from other matters, in an intelligible and easily accessible form.</p> <ul style="list-style-type: none"> The relevant information is revealed to the public by the Data Subject; (Article 5(2)(e)) It is necessary for the institution, usage or protection of a right; (Article 5(2)(f)) It is necessary for the legitimate interests of the data controller, provided that the fundamental rights and freedoms of the Data Subject are not harmed. (Article 5(2)(g)) <p>Note: Explicit consent is defined as “freely given, explicit and informed consent”. (Article 3(a))</p> <p>Special category data The controller must not process special categories of Personal Data without obtaining the explicit consent of the Data Subject except in certain conditions. (Article 6(2))</p> <p>Special Category Personal Data, other than that relating to health and sexual life, may be processed without obtaining the explicit consent of the Data Subject if law permits it. (Article 6(3))</p> <p>Personal Data relating to health and sexual life may only be processed without obtaining the explicit consent of the Data Subject for purposes of public health, operation of preventive medicine, etc. (Article 6(3))</p> <p>The controller must take the adequate measures as designated by the Board when Processing special categories of Personal Data. (Article 6(4))</p> <p>Deletion, destruction and anonymisation Controllers must delete, destroy or anonymise either <i>ex officio</i>, or at the request of the Data Subject when the reasons necessitating their Processing cease to exist. (Article 7(1))</p> <p><i>The Regulation on Deleting, Destroying and Anonymising Personal Data 2017</i> sets out data controllers' obligations regarding the periodic destruction of data, and the</p>	

GDPR	Data Protection Law	General Observations
	<p>The consent must be able to be withdrawn at any time. (Article 24)</p> <p>The controller must make reasonable efforts to verify parental consent (when the child is under 16, although in some members states may be as young as 13).</p> <p>Choosing a data processor The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of this Regulation and ensure the protection of the rights of the Data Subject.</p> <p>Processing by a processor shall be governed by a contract or other legal act. (Article 28)</p> <p>Notifications In the case of a Personal Data breach, the controller must notify the supervisory authority of the breach. This must be done without due delay and, where feasible, not later than 72 hours after having become aware of it. (Article 33)</p> <p>Record keeping Each controller must maintain a record of its Processing activities. (Article 30)</p> <p>Appoint a representative The controller must appoint an EU representative in certain situations. (Article 27)</p> <p>Appoint a DPO The controller must appoint a Data Protection Officer (DPO) in certain situations. (Article 37(1))</p> <p>destruction of data when the purpose for Processing no longer exists.</p> <p>Transfers The controller must not transfer Personal Data without obtaining the explicit consent of the Data Subject unless one of the lawful conditions for Processing in article 5 and/or 6 are met. (Articles 5, 6)</p> <p>Transfers abroad The controller shall not transfer Personal Data abroad without obtaining the explicit consent of the Data Subject, unless one of the conditions in Article 5(2) or Article 6(3) (lawful conditions for Processing without consent) are met, and:</p> <ul style="list-style-type: none"> • The country is deemed to have an adequate level of protection; • The controller in Turkey and the controller abroad, commit to providing an adequate level of protection and the Board gives permission for the transfer. (Articles 5 and 6) <p>Data subject rights The data controller must inform Data Subjects when collecting the Personal Data of:</p> <ul style="list-style-type: none"> • The identity of the data controller and its representative (if applicable); • The purposes of the Processing; • The persons to whom the Personal Data might be transferred and the purposes of this; • The method and legal reason for collecting the data; • The Data Subject rights (as set out below and in article 11). (Article 10(1)) <p>The controller must respond to Data Subject requests as per Article 11 (detailed below). The requests must be dealt with free of charge and within 30 days. (Article 11)</p>	

GDPR	Data Protection Law	General Observations
	<p>Security The data controller shall take all necessary technical and organisational measures to provide an appropriate level of security over Personal Data. (Article 12)</p> <p>Registration Data controller must register with the Data Controllers Registry prior to commencing Processing. The registration must include certain information. (Article 16)</p> <p>The controller must inform the Board of any changes to the above information. (Article 16(4))</p> <p>The Data Controllers' Registry is also regulated by the <i>Regulation on Data Controllers' Registry 2017</i> which provides the principles and procedures for registration with VERBIS (the registry held with the DPA).</p>	
<p>Data Subject Rights</p>	<p>Transparent communication In order to ensure that Personal Data are processed fairly and lawfully, controllers must provide certain minimum information to Data Subjects, regarding the collection and further Processing of their Personal Data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. (Articles 5(1)(a), 12-14)</p> <p>Data subject rights Data controllers have a legal obligation to give effect to the rights of Data Subjects. (Article 12(2))</p> <p>Identifying data subjects Data controllers must not refuse to give effect to the rights of a Data Subject unless the controller cannot identify the Data Subject. The controller must use all reasonable efforts to verify the identity of Data Subjects. Where the controller has reasonable doubts as to the identity of the Data Subject, the controller may request the provision of additional information necessary to confirm the identity of the Data Subject, but is not required to do so. (Article 12(2), (6))</p>	<p>Data subject rights Data Subjects can:</p> <ul style="list-style-type: none"> • Learn if Personal Data regarding him/her has been processed. • Request information about the Processing (if his/her data has been processed). • Learn the purpose of the Processing and whether the data is being processed in accordance with the purpose of collection. • Know the third parties (in the country or abroad) to whom the Personal Data has been transferred. • Request rectification if his/her Personal Data has been processed incompletely or inaccurately. • Request deletion or destruction of Personal Data within the framework of the conditions set out under Article 7 of the Data Protection Law. • Request notification of the rectification or deletion to third parties to whom the Personal Data has been transferred. • Object to the occurrence of any result that is to his/her detriment because of analysis of Personal Data exclusively through automated systems. <p>Being based on the 1995 Directive, the Data Protection Law largely mirrors the GDPR in terms of Data Subject rights. However, the GDPR expands on the rights contained in the 1995 Directive and creates several entirely new rights.</p>

GDPR	Data Protection Law	General Observations
	<p>Time limits A controller must, within one month of receiving a request made under those rights, provide any requested information in relation to any of the rights of Data Subjects. If the controller fails to meet this deadline, the Data Subject may complain to the relevant DPSA and may seek a judicial remedy. Where a controller receives large numbers of requests, or especially complex requests, the time limit may be extended by a maximum of two further months. (Article 12(3) - (4))</p> <p>Basic information Data Subjects have the right to be provided with information on the identity of the controller, the reasons for Processing their Personal Data and other relevant information necessary to ensure the fair and transparent Processing of Personal Data. (Articles 13 and 14)</p> <p>Right of access Data Subjects have the right to obtain the following:</p> <ul style="list-style-type: none"> • confirmation of whether, and where, the controller is Processing their Personal Data; • information about the purposes of the Processing; • information about the categories of data being processed; • information about the categories of recipients with whom the data may be shared; • information about the period for which the data will be stored (or the criteria used to determine that period); • information about the existence of the rights to erasure, to rectification, to restriction of Processing and to object to Processing; • information about the existence of the right to complain to the DPSA; • where the data were not collected from the Data Subject, information as to the source of the data; and • information about the existence of, and an explanation of the logic involved in any automated Processing that has a significant effect on Data Subjects; and 	<ul style="list-style-type: none"> • Request compensation if he/she incurs damage because of the unlawful Processing of his/her Personal Data. (Article 11)

GDPR	Data Protection Law	General Observations
<ul style="list-style-type: none"> Data Subjects may request a copy of the Personal Data being processed. (Article 15) <p>Access fees Data controllers must give effect to the rights of access, rectification, erasure and the right to object, free of charge. The controller may charge a reasonable fee for "repetitive requests", "manifestly unfounded or excessive requests" or "further copies". (Articles 12(5), 15(3), (4))</p> <p>Rectification Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data Subjects have the right to rectification of inaccurate Personal Data. (Articles 5(1)(d), 16)</p> <p>Erasure Data Subjects have the right to erasure of Personal Data if:</p> <ul style="list-style-type: none"> the data are no longer needed for their original purpose (and no new lawful purpose exists); the lawful basis for the Processing is the Data Subject's consent, the Data Subject withdraws that consent, and no other lawful ground exists; the Data Subject exercises the right to object, and the controller has no overriding grounds for continuing the Processing; the data have been processed unlawfully; or erasure is necessary for compliance with EU law or the national law of the relevant Member State. (Article 17) <p>Restrict processing Data Subjects have the right to restrict the Processing of Personal Data (meaning that the data may only be held by the controller, and may only be used for limited purposes) if:</p> <ul style="list-style-type: none"> the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); 		

GDPR	Data Protection Law	General Observations
	<ul style="list-style-type: none"> the Processing is unlawful and the Data Subject requests restriction (as opposed to exercising the right to erasure); the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or if verification of overriding grounds is pending, in the context of an erasure request. (Article 18) <p>Portability Data Subjects have a right to:</p> <ul style="list-style-type: none"> receive a copy of their Personal Data in a structured, commonly used, machine-readable format that supports re-use; transfer their Personal Data from one controller to another; store their Personal Data for further personal use on a private device; and have their Personal Data transmitted directly between controllers without hindrance. (Article 20) <p>Object to processing Data Subjects have the right to object, on grounds relating to their particular situation, to the Processing of Personal Data, where the basis for that Processing is either:</p> <ul style="list-style-type: none"> public interest; or legitimate interests of the controller. <p>The controller must cease such Processing unless the controller:</p> <ul style="list-style-type: none"> demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject; or requires the data in order to establish, exercise or defend legal rights. (Article 21) 	

GDPR	Data Protection Law	General Observations
	<p>Where Personal Data are processed for scientific and historical research purposes or statistical purposes, the Data Subject has the right to object, unless the Processing is necessary for the performance of a task carried out for reasons of public interest. (Articles 21(6), 83(1))</p> <p>Object to direct marketing Data Subjects have the right to object to the Processing of Personal Data for the purpose of direct marketing, including profiling. (Article 21(2) – (3))</p> <p>Duty to inform of right to object The right to object to Processing of Personal Data noted above must be communicated to the Data Subject no later than the time of the first communication with the Data Subject. This information should be provided clearly and separately from any other information provided to the Data Subject. (Articles 3(2)(b), 14(2)(c), 15(1)(e), 21(4))</p> <p>Automated processing Data Subjects have the right not to be subject to a decision based solely on automated Processing which significantly affect them (including profiling). Such Processing is permitted where:</p> <ul style="list-style-type: none"> • it is necessary for entering into or performing a contract with the Data Subject provided that appropriate safeguards are in place; • it is authorised by law; or • the Data Subject has explicitly consented and appropriate safeguards are in place. (Article 22) 	
<p>Cross-Border Transfer Rules</p>	<p>General prohibition Cross-Border Personal Data Transfers may only take place if the transfer is made to an Adequate Jurisdiction or the data exporter has implemented a lawful data transfer mechanism (or an exemption or derogation applies). (Articles 44, 45)</p> <p>General prohibition Personal Data may not be transferred abroad without obtaining the explicit consent of the Data Subject, unless one of the conditions and/or exemptions for Processing in Article 5(2) or 6(3) exist and:</p> <ul style="list-style-type: none"> • The country to which Personal Data is transferred has an adequate level of protection; or 	<p>The rules surrounding cross-border data transfers set out in the Data Protection Law, being based on the 1995 Directive, mirror to a significant extent those in the GDPR. The GDPR however, whilst maintaining the existing data transfer mechanisms created under the 1995 Directive (with some minor amendments), also creates a number of new transfer mechanisms.</p>

GDPR	Data Protection Law	General Observations
	<p>Adequacy decisions Cross-border data transfers may take place if the third country receives an Adequacy Decision from the EU Commission. (Articles 44, 45)</p> <p>The EU Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the USA (subject to compliance with the terms of the US-EU Privacy Shield).</p> <p>Public authorities Cross-border data transfers between public authorities may take place under agreements between public authorities, which do not require any specific authorisation from a DPSA. (Articles 46(2)(a), 46(3)(b))</p> <p>Binding Corporate Rules Cross-Border Data Transfer within a corporate group may take place on the basis of Binding Corporate Rules ("BCRs"). BCRs require approval from DPSAs, but approved, individual transfers made under the BCRs do not require further approval. (Articles 4(20) 46(2)(b), 47)</p> <p>Model clauses Cross-border data transfers may take place on the basis of the Model Clauses entered into between the data exporter and data recipient. Existing Model Clauses implemented under the 1995 Directive remain valid until amended, replaced or repealed under the GDPR. (Articles 28(6)-(8), 46(2)(c), 57(1)(j), (r), 93(2))</p> <p>Other mechanisms Cross-border data transfers may take place on the basis, <i>inter alia</i>, of:</p> <ul style="list-style-type: none"> standard data protection clauses adopted by one or more DPSAs under the GDPR. (Articles 46(2)(d), 64(1)(d), 57(1)(j), (r), 93(2)) 	<p>NOTE: Under the GDPR, cross-border data transfers may take place on the basis of standard data protection clauses approved by the EU Commission ("Model Clauses"). The current set of Model Clauses are currently being challenged as a form of appropriate data transfer mechanism; therefore their future is uncertain.</p> <p>In January 2019, the Irish Supreme Court (as part of the <i>Schrems v Facebook</i> litigation) heard an appeal by Facebook over a decision of the Irish High Court to refer a number of questions to the Court of Justice of the EU ("CJEU") regarding the validity of this data transfer mechanism. The Supreme Court will publish its decision in due course. If Facebook is unsuccessful in its appeal, the CJEU will rule on these questions, which may result in a declaration that the Model Clauses are no longer valid as a transfer mechanism.</p>

GDPR		Data Protection Law	General Observations
	<ul style="list-style-type: none"> an approved code of conduct, together with binding and enforceable commitments to provide appropriate safeguards. (Articles 40, 41, 46(2)(e)) certifications together with binding and enforceable commitments of the data importer to apply the certification to the transferred data. (Articles 42, 43, 46(2)(f)) ad hoc clauses conforming to the GDPR and approved by the relevant DPSA. (Articles 46(3)(a), (4), 63)) administrative arrangements between public authorities (e.g., MOUs) subject DPSA approval. (Articles 46(3)(b), (4), 63) <p>Derogations Cross-border data transfers may be made on the basis, <i>inter alia</i>, that:</p> <ul style="list-style-type: none"> the Data Subject explicitly consents having been informed of the possible risks of such transfer. (Article 49(1)(a), (3)) the performance of a contract between the Data Subject and the controller. (Article 49(1)(b), (3)) it is necessary for the purposes of performing or concluding a contract in the interests of the Data Subject. (Article 49(1)(c), (3)) the transfer is necessary for important reasons of public interest. (Article 49(1)(d), (4)) it is necessary for the purposes of legal proceedings, or obtaining legal advice. (Article 49(1)(e)) the transfer is necessary in order to protect the vital interests of the Data Subject, where the Data Subject is incapable of giving consent. (Article 49(1)(f)) the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by those of the individual subject to informing the relevant DPSA and the Data Subjects. (Article 49(1), (3), (6)) 		
Personal Data Security	<p>Security Data controllers must implement appropriate technical and organisational security measures to protect Personal</p>	<p>Technical & organisational measures Data controllers must take all technical necessary organisational measures to ensure a suitable security level to:</p>	Being based on the 1995 Directive, the Data Protection Law leaves a significant amount of discretion to the controller in terms of the technical and organisational measures to be implemented in the controller's particular

GDPR		Data Protection Law	General Observations
	<p>Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.</p> <p>Depending on the nature of the Processing, these measures may include:</p> <ul style="list-style-type: none"> • encryption of the Personal Data; • on-going reviews of security measures; • redundancy and back-up facilities; and • regular security testing. (Article 32) 	<ul style="list-style-type: none"> • Prevent Personal Data from being processed unlawfully. • Prevent Personal Data from being accessed unlawfully. • To ensure the protection of Personal Data. (Article 12) <p>Joint liability When another natural or legal person processes Personal Data on behalf of the data controller, the data controller shall be jointly liable with such persons with regard to taking the appropriate security measures. (Article 12(2))</p> <p>Additional measures for sensitive personal data As per the Turkish Data Protection Authority's (DPAs) <i>Decision No 2018/10 of 2018</i>, additional measures must be taken for Processing sensitive Personal Data in Turkey. These include:</p> <ul style="list-style-type: none"> • Data controllers must establish a manageable and sustainable policy and procedure with clearly defined rules specific for the security of sensitive Personal Data. • Precautions for employees who process sensitive Personal Data. • Precautions specific to the Processing of sensitive Personal Data in electronic media. • Precautions specific to the Processing of sensitive Personal Data in a physical environment. • Precautions specific to the transfer of sensitive Personal Data. 	<p>context. The GDPR is more prescriptive but the net effect is very similar.</p>
Administrative Fines and Regulatory Sanctions	<p>Judicial remedies Data Subjects have the right to an effective judicial remedy against:</p> <ul style="list-style-type: none"> • decisions of a DPSA concerning them; • any failure by a DPSA to deal with, or respond to, a complaint within three months; and 	<p>Criminal sanctions The Turkish Criminal Code applies for non-compliance with data protection laws. (Article 17)</p> <p>Persons who illegally collect Personal Data may be subject to imprisonment for a term of between 1 and 3 years. If the Personal Data is sensitive Personal Data, imprisonment may be for a term between 1.5 - 4.5 years. (Article 135, Criminal Code)</p>	<p>Whereas the remedies and sanctions available under the Data Protection Law are comparatively low, the remedies and financial sanctions available to DPSAs under the GDPR are significantly greater save for the imprisonment sanctions.</p> <p>Under the GDPR, DPSAs are considered to have more significant enforcement powers.</p>

GDPR	Data Protection Law	General Observations
	<ul style="list-style-type: none"> any unlawful Processing of their Personal Data by a controller or processor. (Article 78-79) <p>Compensation & liability A Data Subject who has suffered harm as a result of the unlawful Processing of his or her Personal Data has the right to receive compensation from the controller or processor for the harm suffered:</p> <ul style="list-style-type: none"> Any controller involved in the Processing is liable for the harm caused. A processor is liable for the harm caused by any of its (or its sub-processor's) Processing activities that are not in compliance with its obligations under the GDPR, or are in breach of the controller's instructions. To ensure effective compensation, each controller or processor will be held liable for the entirety of the harm caused, if they are involved in the same Processing and responsible for that harm. (Article 82(1)-(2), (4)) <p>Joint-controller liability Data Subjects are entitled to enforce their rights against any of the joint controllers. Each joint controller is liable for the entirety of the damage, although national law may apportion liability between them. If one joint controller has paid full compensation, it may then bring proceedings against the other joint controllers to recover their portions of the damages. (Article 26(3), 82(3)-(5))</p> <p>Exemptions from liability A controller or processor is exempt from liability if it proves that it is not responsible for the event giving rise to the harm. There is no mention of force majeure events. (Article 82(3))</p> <p>Administrative fines The maximum fine that can be imposed for serious infringements of the GDPR is the greater of €20 million or 4% of an undertaking's worldwide turnover for the preceding financial year. (Article 83(5) – (6))</p>	<p>Persons who illegally transfer Personal Data or make Personal Data available to the public may be subject to imprisonment for a term between 2 - 4 years. (Article 136, Criminal Code)</p> <p>If any of the above criminal acts are used as a result or advantage of a professional position, or by a public officer using the authority given to them, the sanctions will be increased by 50%. (Article 137, Criminal Code).</p> <p>Failing to delete data once the retention period has expired can be punishable by between 1 - 2 years imprisonment. (Article 138 Criminal Code)</p> <p>Administrative fines Failure to comply with the 'information notice' requirements can lead to a fine of between TRY 5,000 – TRY 100,000. (Article 18)</p> <p>Failure to comply with the data security obligations can lead to a fine of between TRY 15,000 and TRY 1 million. (Article 18)</p> <p>Failure to comply with the requirements regarding the Data Controllers' Registry can lead to a fine of between TRY 20,000 and TRY 1 million. (Article 18)</p>

GDPR		Data Protection Law	General Observations
	<p>Fine criteria</p> <p>When deciding whether to impose a fine and deciding on the amount, DPSAs are required to give due regard to a range of issues, including:</p> <ul style="list-style-type: none"> • the nature, gravity and duration of the infringement; • the number of Data Subjects affected and the level of harm suffered by them; • the intentional or negligent character of the infringement; • any action taken by the controller or processor to mitigate the harm; • any relevant previous infringements by the controller or processor; • the degree of co-operation with the relevant DPSA; • whether the infringement was self-reported by the controller or processor; and • any other aggravating or mitigating factors. (Article 82(3)) 		
<p>Role and Powers of any relevant Data Protection Supervisory Authority</p>	<p>Independence</p> <p>DPSAs must act independently and operate free from all outside influences, including government control. (Article 52)</p> <p>Tasks</p> <p>The tasks of DPSAs include obligations to:</p> <ul style="list-style-type: none"> • monitor and enforce the application of the GDPR; • promote awareness of the risks, rules, safeguards and rights pertaining to Personal Data (especially in relation to children); • advise national and governmental institutions on the application of the GDPR; • hear claims brought by Data Subjects or their representatives, and inform Data Subjects of the outcome of such claims; • establish requirements for Impact Assessments; • encourage the creation of Codes of Conduct and review certifications; • authorise Model Clauses and BCRs; 	<p>Personal Data Protection Authority</p> <p>The national data protection authority is the Personal Data Protection Authority. (Article 19)</p> <p>Personal Data Protection Board</p> <p>The Personal Data Protection Authority's decision-making body is the Personal Data Protection Board. (Article 19(4))</p> <p>Regulation of powers</p> <p>The organisational structure of the Authority and the duties and powers of its bodies are regulated under the Regulation on the Organisation of Personal Data Protection Authority and the Regulation on the Working Procedures and Principles of Personal Data Protection Board.</p> <p>Duties and powers of the Authority and Board</p> <p>The powers and duties of the Authority and Board include:</p> <ul style="list-style-type: none"> • Drafting the secondary legislation regarding data protection. 	<p>Under the GDPR, DPSAs are considered to have more significant supervisory and enforcement powers.</p>

GDPR		Data Protection Law	General Observations
	<ul style="list-style-type: none"> • keep records of sanctions and enforcement actions; and • fulfil "any other tasks related to protection of Personal Data". (Article 55, 57) <p>Powers DPSAs are empowered to oversee enforcement of the GDPR, investigate breaches of the GDPR and bring legal proceedings where necessary. (Article 58)</p>	<ul style="list-style-type: none"> • Maintaining the register of Data Controllers (the Data Controllers' Registry) • Ensuring Personal Data is processed in accordance with fundamental rights and freedoms. • Deciding on decisions regarding complaints by Data Subjects. • Examining whether Personal Data has been processed according to the law. • Where a complaint is filed or an alleged violation of the law has occurred, take temporary measures to stop such violation where necessary. • Determine sufficient measures for the Processing of sensitive Personal Data. (Article 20 and 21) 	

This report was produced by PwC Legal Middle East on behalf of the GSMA. It was produced as a contribution to public debate in MENA and neither PwC nor PriceWaterhouseCoopers Legal Middle East LLP accept any duty of care, responsibility or liability whatsoever for any loss or damage suffered or costs incurred by any party or person arising out of or in connection with the information contained in this report or for any decision based on it or related to it.