QATAR

Law and Practice

Contributed by:
Alex Saleh, Feras Gadamsi, Yousef Al Amly and Rana Moustafa
GLA & Company

Contents

GLA & Company is a regional MENA-based law firm with offices in Dubai, Abu Dhabi, Riyadh, Kuwait, Cairo and Beirut. It provides strategic, cost-effective and forward-thinking legal representation for companies seeking to do business in the Middle East. The firm boasts a diverse portfolio of clients, ranging from start-ups to global enterprises doing business in the Middle East. GLA's practice consists of a full-service law firm that handles everything from simple advisory work to complex contentious and non-contentious matters. With extensive experience advising clients in the key Gulf Cooperation Council (GCC) states of Kuwait, Saudi Arabia, Qatar and the United Arab Emirates (UAE) – as well as in Egypt and Lebanon – the firm offers unique insights for companies seeking quality legal services. Data protection and privacy, in particular, is a key focus area for the firm, considering the expansion and revamping of applicable laws and regulations across the GCC.

Authors

Alex Saleh is a founder and managing partner of GLA & Company and takes a leading regional role in the firm's M&A and private equity practice. With more than 25 years of experience in both the Gulf Cooperation Council and the USA, he has accumulated sizeable expertise in the areas of banking and finance, M&A, capital market deals and infrastructure projects. His experience garners praise from the leading legal directories and his transactions are regularly noted by the same institutions and organisations.

Feras Gadamsi is a partner based in the firm's Dubai office, leading GLA & Company's global technology, data and privacy practice. Feras also advises on compliance issues, including regional anti-bribery and anti-corruption laws, US FCPA, internal investigations, and audits. He started his career in private practice as an associate at Bracewell in Houston before moving to Dubai with King and Spalding. Immediately prior to joining the firm, Feras served as Regional General Counsel at IBM. He was formerly Uber's lawyer in the MEA region, serving as General Counsel for Middle East and Africa, Oracle Cerner's Regional General Counsel, and served as CLO and Head of Policy for a Dubai-based start-up.

Yousef Al Amly is a partner at GLA & Company, and is a dual-registered lawyer and certified practitioner in both the UK and Egypt. With accumulated years of experience in corporate, banking and finance, equity capital markets, and debt capital markets, Yousef has advised clients on complex corporate and commercial structures and transactions in relation to joint ventures, corporate restructuring, M&A, equity capital markets and commercial transactions (including franchise, distributorship and agency); and has advised high-profile companies in the Middle East on anti-money laundering means, cybersecurity and data protection. Yousef is a member of the UK Solicitors Regulatory Authority, the Egypt Bar Association, and the Egyptian Court of Appeals.

Rana Moustafa is an associate at GLA & Company with extensive experience in international and domestic commercial disputes. Rana's experience spans across the GCC and Europe, representing clients in Kuwait, Lebanon, Qatar, United Arab Emirates, Saudi Arabia, Egypt and France. She has experience in international and domestic arbitration, working on matters held under the auspices of ICC/DIFC-LCIA/CRCICA/DIAC/ICSID and CAS. Rana extended her experience in data protection while working on matters related to data protection disputes, data protection framework at the workplace and data protection policies for clients. She is a member of the Egypt Bar Association and is currently studying for the French Barreaux.

GLA & Company

Alex Saleh
Managing Partner

Tel: Kuwait +(965) 669 55516
UAE +(971) 54 997 4040
Email: alex.saleh@glaco.com
Web: www.glaco.com/attorneys/alex-saleh/

1. Basic National Regime

1.1 Laws

Qatar introduced Qatari Law No 13 of 2016 (the "Personal Data Privacy Protection Law", or PDPL), which took effect in 2017. Qatar was the first country in the Middle East to introduce a dedicated onshore data protection and privacy law. The Compliance and Data Protection Department (CDP) attached to the Ministry of Transport and Communications (MOTC) published guidelines concerning the PDPL (the "Guidelines") in 2021 with the aim of frameworking data protection in Qatar. The PDPL applies to personal data that is received, collected, extracted, and/or processed through electronic or traditional methods. The PDPL aligns with the universal data protection principles, which were established as the core of the General Data Protection Regulations (GDPR) of the European Union.

The fundamental data protection provisions are aligned with the telecommunications law promulgated by Decree Law No 34 of 2006 in the state of Qatar, the Electronic Transactions and Commerce Law promulgated by Decree Law No 16 of 2010, Law No 2 of 2011 on Official Statistics (as amended by Law No 4 of 2015) and the Cybercrimes Combating Law promulgated by Law No 14 of 2014. Qatar's data protection and privacy regime is comprised of provisions related to penalties in other laws such as the penal code, the Trade Secrets Law, the Qatar Constitution, the Labour Law, and the Qatar banking regulations issued by the Qatar Central Bank (QCB).

The Data Protection Office (DPO) is an independent institution of the Qatar Financial Centre (QFC). The QFC first started enacting the data protection law in 2005. It is charged with administrating the QFC Data Protection Regulations 2021 (the "Regulations") and all aspects of data protection within the QFC.

On the other hand, Qatar adopted a national artificial intelligence strategy in early 2022, which is implemented in line with the country's 2030 vision. As a driver for innovation, the MOTC approved the outline of the strategy in 2019; the main goal behind it was furnishing sustainable and innovative economic growth, by targeting six main pillars in the state of Qatar – education, data access, employment, business, research, and ethics.

Further, the Qatar Communications Regulatory Authority (CRA) recently issued, in 2022, the Cloud Policy Framework to enable the transition to a fully digitalised nation.

1.2 Regulators

The Compliance and Data Protection department at the MOTC constitutes the key regulator in Qatar along with the National Cyber Security Agency (NCSA), which is the competent department for administration and enforcement of the PDPL. It is the key authority conducting investigations regarding cybersecurity issues, implementing and examining issues related to national cyber-risks, and conducting fieldwork solidifying resilience against cybercrimes and crises.

The DPO is concerned with the data protection framework for QFC since 2021. It is the institution charged with providing guidance on all data protection matters or complaints related to the Regulations. The DPO is concerned with the protection of the rights of individuals and ensuring implementation of protection measures for all QFC entities, firms or future investors.

1.3 Administration and Enforcement Process

Administration

The enforcement process usually is triggered by a complaint filed before the MOTC, which is the competent authority in the state of Qatar. The MOTC will embark on an investigation process in order to verify the veracity of the complaint and thereafter, if warranted, issue a judicial order binding the controller or processor in line with its powers under the law.

Enforcement Process: Search, Investigate and Seize

The MOTC will issue a rectification decision, ordering the violating entity to rectify the violation within a fixed period, as per Article 26 of the PDPL. The controller or processor has the right to file a "grievance" against such order to the minister within 60 days from the date of notification. The decision issued by the minister related to such grievance shall be deemed final according to Article 26 of the PDPL. The judicial officers and/or law enforcement officers designated by the MOTC have the power according to Article 29 of the PDPL to seize and document any crimes related to violating the provisions of the law.

Furthermore, at the QFC level, if the QFC DPO examines a contravention or violation of the law by any data controller, a direction would be issued to the data controller, addressing it to undertake the following, in compliance with Article 22 of the Regulations:

- to act or omit from doing any step; and
- 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.

1.4 Multilateral and Subnational Issues

The national Qatari system inherently relates to the GDPR in the EU and broadly follows the general principles established in the European Union Data Protection Directive (Directive 95/46/EC) and the General Data Protection Regulations (GDPR). It should be noted that in respect of the GDPR's application vis-à-vis Qatari entities that have operations or establishments in the European Union (EU), their data processing activities will be subject to the GDPR irrespective of whether the processing takes place in the EU.

1.5 Major NGOs and Self-Regulatory Organisations

The Gulf Centre for Human Rights (GCHR) is an independent, non-profit CSO founded in April 2011 that works on promoting human rights, including the freedoms of association, peaceful assembly, and expression. During its second universal periodic review cycle in 2014, Qatar received 12 recommendations pertaining to free expression, free press, and the right to privacy. Amnesty International's Security Lab led an investigation in 2020 into the efficacy of Ehteraz, the coronavirus tracker application, identifying "critical weaknesses" in its security system, compromising sensitive data related to the health and confidential information of many citizens.

In November 2014, Qatar's MOTC announced a new "Open Data Policy" that aims to create an open and transparent platform where processing, sharing and interpreting information is accessible. The policy is intended to make "non-personal government data" such as crime figures available to the public, and it also institutes a mechanism through which citizens may request information.

With the Qatari focus on adopting legislation and collaborating with regional players for the implementation of data privacy, an Information Communications Technology (ITU) Regional Workshop for Cyber Security and Critical Infrastructure Protection (CIIP) and Cyber Security Forensics Workshop was held in Doha in February 2008. The workshop was focused on addressing threats in cyberspace and developing appropriate tools to combat cyber-attacks. This issue was also discussed in the 15th GCC e-government and e-services forum which was held in Dubai in May 2009.

In the state of Qatar, there has also been a growing focus on the incorporation of artificial intelligence training for judges and interest in teaching lawmakers about the rule of law's connection to artificial intelligence. This has been promoted in Qatar by UNESCO in 2022.

1.6 System Characteristics

DPL: Mirroring the GDPR

There is an inextricable link between DPL and GDPR, with enforcement in Qatar becoming more effective with the passage of many cross-laws related to privacy and data protection, the aim being to stand alongside peer jurisdictions following the same EU omnibus model.

QFC System of DPL

The Regulations for QFC aim to ensure proper monitoring and regulation of QFC firms in the context of data protection. Some of the most significant amendments introduced in those Regulations, including the establishment of eight main principles in the context of processing personal data, mirror those found in the GDPR. The Regulations are inspired by the privacy and data protection principles and guidelines contained in the EU Directive and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The enforcement measures under the DPL are highly similar to those of the EU Directive; however, the enforcement and sanctions at the QFC level still lack considerable appropriations as compared with the EU GDPR.

1.7 Key Developments

The key changes made to the QFC Regulations in 2021 pave the way for core innovations in data privacy in the state of Qatar. The updates to the law allowed the MOTC to hold companies to higher standards and impose significant fines in the event of non-compliance. Moreover, the updates introduced purpose specification, data minimisation, new rights, and additional transparency for controllers, which highlighted the Qatari competitive position with other international enforcement and regulatory bodies. Thus, it is becoming easier and more flexible for a large range of companies to safely store their data locally and facilitate operations on local cloud servers.

Another key development is clothed in terms of discussions around the assessment of adequate jurisdiction, after Schrems II. Now, following Schrems II, QFC data controllers are considering the Privacy Shield and all the other circumstances around their data transfers to the US.

Currently, one of the main topics still attracting public attention is related to the Qatari government's direct access to citizens' data.

1.8 Significant Pending Changes, Hot Topics and Issues

Pending Changes

Currently, there is no freedom of information legislation in the state of Qatar, a step being discussed by most practitioners. In the same vein, the focus is on organisations and employers who would need to display that permission was duly

received from employees for the assessment and collection of their personal sensitive and classified data.

Another pending change that is the subject of recent discussion, since the introduction to the market of start-ups in the artificial intelligence (AI) industry, is the development of a legal framework that complies with the recent evolution in the AI industry and its upcoming inclusion in all aspects of life.

Critical Discussions

Another key hot topic throughout 2022 was the FIFA World Cup held in Qatar and data privacy. Many European regulators stated that the accommodation application Hayaa used during the World Cup and the coronavirus tracking application Ehteraz were based on data collection and collection of metadata protected by secrecy laws in Germany, France and other European countries. Other examples of current issues include the collection of information regarding COVID-19 vaccinations, psychology tests and IQ tests.

One of the critical discussions now being held between practitioners is the credibility of AI usage in the state of Qatar and specifically the legal framework and legal ethics that must be construed in order to guarantee the good use of such a modern tool, specifically in the areas of healthcare and employment.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

Requirement for Appointment of Privacy Protection Officers

The DPL does not provide for an express obligation falling upon organisations in Qatar to appoint a data protection officer. Nevertheless, there is an obligation on the data controller to specify processors responsible for protecting personal data, train them appropriately on the protection of personal data and raise their awareness in relation to protecting personal data.

Criteria Necessary for Collection and Processing

The collection and processing of data must be conducted in compliance with the PDPL. The controller is bound to process data honestly and legally. The criteria followed for collection and processing of data in the state of Qatar is based on the principle of consent. The data controller or any other party who is conducting data processing is obliged to provide a lawful purpose for which the data is being processed; describe specifically the activities and the degrees of disclosure of personal data and any other information deemed necessary and required for the satisfaction of personal data processing. Those obligations align with the provisions stipulated in Articles 13 and 8 of the PDPL.

An individual may, at any time, have access to their personal data and request its review, in the face of any observer. In the same vein, any individual whose data is being processed or collected has the right to require and obtain from the data controller upon request, at reasonable intervals and without excessive delay or expense a confirmation as to whether personal data relating to them is being processed and, if

so, information at least as to the purposes of the processing, the categories of personal data concerned and the recipients or categories of recipients to whom the personal data is disclosed. Other than mentioned above, no person may request access to any personal information held by an authority other than their personal data.

A practical example explaining the criteria necessary for collection and processing is the recently discussed example of the collection and tracking of points of players, their movements and positioning during the FIFA World Cup 2022. According to the PDPL, this is considered as processing. However, even if the GDPR and the PDPL require prior express consent, an examination has concluded that, in the context of the FIFA World Cup, the players have impliedly consented to the processing of such personal data by the World Cup organisers.

Henceforth, the criteria are based on prior express consent but in certain circumstances (as mentioned above) the collection and processing may be drawn in the context of an implied consent.

Application of the "Privacy by Design and by Default" Concept

The DPL requires controllers to implement appropriate administrative, technical and financial precautions to protect personal data. These precautions must be proportionate to the risk of serious damage to individuals. This is known as Data Privacy by Design and by Default. Data controllers are currently invited to integrate privacy tools and techniques in their processing activities and practices, starting from the design stage, throughout the life of the activity. The best-known example would be the approach provided by data controllers, requiring individuals to opt-in not opt-out.

Furthermore, Data Protection Impact Assessment (DPIA) and a Record of Personal Data Processing are a key component of any Personal Data Management System. This aligns with the provisions in Articles 13 and 11(1) of the PDPL.

In the state of Qatar, the protection of personal data based on the "privacy by design" concept requires the organisation or entity to implement or use built-in products and systems that are considered as privacy friendly and protecting the personal data of each concerned individual.

Implementation of Internal/External Policies and Data Subject Rights

According to the DPL and Guidelines issued in the state of Qatar, organisations and controllers are bound to implement policies and procedures to enable individuals and data subjects to exercise their rights, including the right to withdraw consent and to request erasure or correction of personal data. Data controllers have 30 days to respond to such requests.

Data Subject Rights

It is provided in the DPL in the state of Qatar that the data controller should ensure that the data collected is:

- being processed fairly, lawfully and securely;
- being 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;
- adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed;
- accurate and, where necessary, kept up to date; and
- 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 it is further processed.

Fairness and Impact Analysis

The Guidelines issued in the state of Qatar provide for a Data Protection Impact Assessment (DPIA) before undertaking any processing activities. This would be applicable in the circumstances where special or sensitive data is being processed or exported. Organisations could be subject to a fine of QAR1 million (USD275,000) for failing to carry out a DPIA. Moreover, the PDPL provides in Article 3 that data processing must be in conformity with the law and principles of good faith. A request permit from the CDP at the MOTC should be submitted and it should identify both permissible grounds and "additional conditions" for processing.

In addition, the Guidelines define the process for obtaining a permit. Data controllers should fill out the "Special Nature Processing Request Form", which must be submitted to the CDP. In the same vein, data controllers will need to submit the relevant DPIA and any other additional information that the CDP may request. Currently, such documents are submitted by email. However, an online portal that would facilitate such submissions is expected to be launched soon.

The Definition of Harm to National Privacy and Data Protection Under the PDPL

A personal data breach means a breach of security leading to the unlawful or accidental alteration, destruction, loss, unauthorised disclosure of, or access to, personal data. This includes both accidental or incidental and deliberate breaches.

The following are examples of harm or breaches classified as violations to data subject rights:

- theft or loss of IT equipment containing personal or business sensitive data;
- inappropriately accessing personal data about customers/staff;
- leaving confidential/sensitive files that may contain personal data unattended;
- inadequate disposal of confidential files that may contain personal data material;
- unauthorised disclosure of client data; and
- using client data for personal gain.

Personal data breaches often result in adverse impact(s) being suffered by individuals, organisations and/or communities, such as:

- compromised personal safety or privacy;
- the burden of additional legal obligation(s) or regulatory penalty(ies);
- financial loss/commercial detriment;
- disruption to business or reputational damage; and
- the inability of individuals to access their data or exercise rights under privacy laws.

The above examples are not exhaustive but are indicative of the types of breaches and consequences against which controllers must put precautions in place for purposes of prevention and mitigation.

2.2 Sectoral and Special Issues

Sensitive or Special Data

The PDPL in the state of Qatar addresses the concept of sensitive personal data, first introduced in the realms of the European Union in its framework on data protection and human rights. The PDPL specifically defines sensitive date as any data consisting of information as to a natural person's:

- ethnic origin/race;
- health;

- physical or mental health or condition;
- religious beliefs;
- relationships/marital status;
- criminal records; and
- children.

This category of "special" personal data is not available for processing except with the permission of the MOTC.

The PDPL does not apply to personal data that is used as statistical data and may also not apply to personal data that is processed in private or family settings. Furthermore, the QFC Regulations provide for a definition of sensitive data to encompass data relating to criminal convictions as well as biometric and genetic data.

The QFC Regulations further stipulate that there must be a particular and specific permit for the processing of sensitive data. According to Article 12 of the Regulations, it is stated that the data controller must apply in writing to the DPO setting out:

- the identity and contact details of the data controller;
- the name, address, telephone number and email address of the person within the data controller responsible for making the application for the permit;
- a description of the processing of sensitive personal data for which the permit is being sought, including a description of the nature of the sensitive personal data involved;
- the purpose of the proposed processing of the sensitive personal data;
- the classes of data subjects being affected;
- the identity of any person to whom the data controller intends disclosing the sensitive personal data;
- to which jurisdictions, if known, such sensitive personal data may be transferred outside the QFC; and
- a description of the safeguards put into place by the data controller, to ensure the security of the sensitive personal data.

Special Overview of Children's Websites

The PDPL obliges all operators of websites targeting children to post specific notifications to the users. Thus, the prior explicit consent of a child's guardian would be taken. Despite the broad coverage of such websites, this is widely viewed in practice as engulfing various categories of digital media, including social media applications.

Internet and Online Streaming

Moreover, as regards the internet and online streaming, the PDPL along with the Qatari Civil code provide for a clear restriction against hate speech (and provide for its defusal), any propaganda that concerns political ties or any disrespect against the Emir or any other political or governmental figure or any religious figure.

Specific Overview of Banking Sector

Banks operating in Qatar must take into consideration precautionary measures as follows:

- raising awareness internally and amongst its service providers;
- conducting due process and reviewing internal policies, disclaimers, consents or agreements and ensuring their compliance with the PDPL;
- conducting marketing and implementing technical support mechanisms able to answer any customer concerns;
- conducting regular training and keeping employees up to date; and

- reviewing all security measures implemented by the bank and the service providers and assessing whether any further steps can be taken or investments be made to protect customer data.

Specific Overview of QFC

The Regulations enhance the rights of data subjects with respect to their personal data as follows:

- right to withdraw consent;
- right to data portability; and
- right not to be subjected to a decision that is based solely on automated processing.

Specific Overview of Health Sector and Private Health Data

Private health data under Article 16 of the PDPL includes personal information related to an ethnic group, children, physical and mental health or state, treatment, health security, cause of death, socio-economic parameters regarding health and wellness, historical healthcare backgrounds such as diseases or any related information, and personal information collected to provide health services and opinions. The consent of individuals, children's guardians, or any individual whose medical coded clinical data is being processed, first must be obtained explicitly or by confirmation.

Cookies

According to the DPL Guidelines, controllers may use "cookies" on the individual's web browser to target direct advertisements messages towards the individual. Such cookies should be deployed only after the individual has "opted-in", ie, has clicked "accept" to allow such direct marketing cookies to be deployed on the individual's browser.

Controllers may collect individuals' email addresses on a web page of the controller's website. The controller must make it clear, on the web page, that if the individual provides their email address in that instance, they are providing their consent towards receiving direct marketing emails until they withdraw their consent.

2.3 Online Marketing

Prohibitions and Limits

The PDPL under Article 22 and within its Guidelines prohibits explicitly unsolicited direct marketing or marketing communications. Prior consent to send electronic marketing communications is required including by wired or wireless communication. The PDPL recognises that the consent must be explicit and unambiguous. It is worth noting that implied consent is not recognised under the PDPL and mostly will be deemed invalidly taken.

The following information must be included in all communications electronically shared:

- the identity of the sender;
- an indication that the message is sent for a purpose of direct marketing;
- a reachable and searchable address; and
- a communication platform enabling the customer to request withdrawal of its consent and complete seizure of all upcoming communications.

Constraints on Behavioural and Targeted Marketing

The guidelines issued in 2020 provide that the Record of Processing Activities (ROPA) is an important record to be implemented since it covers compliance with personal data in marketing requirements. These requirements vary between the following:

- tracking consent of the users/customers/service takers;
- communicating notices and managing privacy in general; and
- monitoring data breaches and notifications.

In the same vein, according to Article 23 and/or Article 24 of the PDPL, it is stipulated that a data controller could be obliged to compensate any damaged individual for any breach of privacy conducted with a fine. And as per the QFC Data Protection Regulation, a data subject has the right to be informed before personal data is disclosed for the first time to third parties or used on their behalf for direct marketing and to be expressly offered the right to object to such disclosures or uses.

2.4 Workplace Privacy

According to the PDPL, workplace privacy rules are strictly providing for a solid framework protecting the employee's privacy. Thus, organisations must provide proof or evidence that they have a permitted reason as well as an additional condition to process their employees' personal data (SISCO systems, telephone or PC monitoring, GPS). Employers will also need to conduct DPIAs when processing employees' personal data as this is considered an example of processing that "may cause serious damage" by the CPD.

The Ministry of Administrative Development, Labour and Social Affairs (MADLSA), on 24 May 2021, launched the first phase of the Unified Platform for Complaints & Whistle-blowers. Through the electronic platform, citizens, expatriates and establishments can file a complaint against entities subject to the provisions of Qatar Labour Law No 14 of 2004 and the Domestic Workers Law promulgated by Law No 15 of 2017 or entities with business regulated by the Ministry of Administrative Development, Labour and Social Affairs.

2.5 Enforcement and Litigation

Process and Complaints Submissions

The Guidelines clarify that required notifications of data breach incidents (to the CDP and affected individuals) must be made within 72 hours. There is currently no requirement in Qatar for data controllers who process personal information to register with the regulator, the NCGAA.

In Qatar, in the event a violation of the DPL occurs, the data subject may file and submit a complaint before the NCGAA. The NCGAA is the competent enforcement authority, and it will investigate the complaint. In the event the complaint is found to be valid, the NCGAA can oblige the data controller or processor to rectify the violation within a specified period.

Potential Enforcement Penalties

As per the DPL, without prejudice to any more severe penalty stipulated by another law, whoever violates any of the provisions of Articles 4, 8, 9, 10, 11 shall be charged with a fine not exceeding QAR1 million (by virtue of Articles 12, 14, 15, 22 of this law). And whoever violates any of the provisions of Articles 13, 16 (third paragraph), 17 of this law shall be charged with a fine not exceeding QAR5 million.

Additionally, the violating legal entity shall be charged with a fine not exceeding QAR1 million if one of the crimes stipulated in this law is committed in its name and for its account, without prejudice to the criminal responsibility of the natural person affiliated to it.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

The laws and standards applicable to law enforcement access to data for serious crimes are similar to the GDPR, and the definition of sensitive personal data now includes data relating to criminal convictions as well as biometric and genetic data. Access to data for serious crimes may be carried out by the agency upon judicial approval without obtaining the consent of the concerned individual or entity.

3.2 Laws and Standards for Access to Data for National Security Purposes

Legal Framework

The state of Qatar has put in place the National Cyber Security Strategy (NCSS), which is essentially a platform for the protection and safeguarding of national interests and rights. The National Information Assurance policy and the National ICS security standard guide security controls and practices to provide protection. Qatar's cyber-prevention law bans offences committed through the internet and IT networks, and is a major technology regulation that must be put into consideration by tech companies.

Operational Framework

The Qatari computer emergency response team (Q-CERT) promotes the identification and prevention of cyber-attacks in the government and critical sectors. The state-of-the-art facilities, infrastructure and financing support systems for technology-based companies, programmes and start-ups.

Access to Data

Certain exemptions under Article 18 apply to all competent authorities in the State of Qatar. A competent authority is any central or local government agency or authority; government entity, organisation, association, or agency owned in whole or part; tribunal, court or regulatory or other agency; as well as any pool of assets owned or sponsored by central or local government or as otherwise prescribed in Qatar law or the Guidelines.

The agencies directly connected to the government and intelligence bodies may have direct access to data without judicial approval. This constitutes one of the main privileges for governmental bodies in the state of Qatar. However, if the above-mentioned bodies carry out the processing of such information, they must still abide by all other obligations under the DPL, such as maintaining a record where the data achieving the aforementioned purposes shall be entered. The conditions, controls and statuses of entry on such record shall be specified by virtue of a decision issued by the Minister.

The authors have yet to examine the cybersecurity measures taking effect in the Qatari jurisdiction, specifically relating to the use of AI to analyse publicly available data to infer security threats.

3.3 Invoking Foreign Government Obligations

The Communications Regulatory Authority (CRA) of Qatar released the Cloud Policy Framework in June 2022. Qatar is not yet a participant in a Cloud Act agreement with the USA. It is anticipated that Qatar will enter into agreements with trusted foreign countries to facilitate the cross-border transfer of non-personal data when these foreign countries are subject to adequate data protection and cybersecurity standards.

However, with the Qatari vision for 2030, the state and CRA would be implementing a cloud-friendly environment where security levels shall be defined by the data owners based on the level of confidentiality, integrity and availability. It is anticipated that encryption keys shall be stored and managed by the data owner for all government-classified data.

3.4 Key Privacy Issues, Conflicts and Public Debates

The governmental entities in Qatar, like many countries and jurisdictions, have access to citizens' and individuals' personal data. As a precautionary measure, and to comply with global standards, governmental entities or agencies would usually have the discretion to use or transmit or process any information acquired. However, the information shared or processed would be classified as confidential.

In the same vein, the governmental entity's employees and officers are obliged to refrain from disclosing any such information or using it in any other way than to undertake their duties (eg, the Hookomi website provides this as a notice to all users). The government's access to data constituted a critical discussion amongst practitioners in Qatar during the collection and processing of data by government applications in relation to world cup fans.

It is noteworthy that one of the key assets of telecoms law in the state of Qatar is that it provides under Article 69 that any person who, in the course of their employment in the telecommunications field, or as a result thereof:

- 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; or
- divulges any information concerning users of telecommunications networks or their communications that are made or received, without legal authority,

shall be subject to an imprisonment penalty for not more than one year and/or a fine of up to QAR100,000.

4. International Considerations

4.1 Restrictions on International Data Issues

Transborder data flow is defined under the DPL as accessing, viewing, retrieving, using or storing personal data without borders constraints. The DPL in the state of Qatar provides that data controllers should not take measures or adopt procedures that may restrict or prevent transborder data flow, unless processing such data violates the provisions of the DPL or will cause gross damage to the data subject.

More specifically, the law reserves the right for governmental bodies to determine that this principle, amongst others, does not apply to certain categories of data they process, based on the following grounds:

- national security;
- international relations;
- the economic or monetary interests of the state; or
- the prevention or investigation of criminal offences.

4.2 Mechanisms or Derogations That Apply to International Data Transfers

A transborder data flow may occur where the data exporter is:

- 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; or
- collecting information to investigate a crime when requested by officials.

Qatar is yet to enter into Mutual Legal Assistance Treaties (MLATs) or bilateral treaties to ensure appropriate involvement of the authorities in the countries where the data is stored.

4.3 Government Notifications and Approvals

The situation where a notification or approval would most likely be required to transfer data internationally or to carry out cross-border transfer would be in the context of QFC transfers. In principle, QFC does not maintain a list of "adequate" jurisdictions. However, in certain circumstances, when the recipient in a country is not deemed to have an adequate level of protection for personal data, it would essentially require obtaining a permit for the transfer and the data controller would apply certain safeguards in accordance with Article 10(1)(a) of the QFC PDPL.

4.4 Data Localisation Requirements

From an operational perspective, according to the CRA it is no longer necessary for data to be stored "on-premises" or "locally". Instead, organisations should implement security measures such as encryption, anonymisation and aggregation at predefined secure hubs (regions/availability zones), which are more efficient than localisation. According to the Cloud Policy Framework issued in the state of Qatar, data residency shall no longer be a requirement as data classification schemes, security and encryption technologies now secure a high level of protection controls.

4.5 Sharing Technical Details

The independent audit reports must verify that Cloud Service Providers (CSP) adhere to security controls and international standards such as ISO 27001, ISO 27018, SOC 1, SOC 2, SOC3, FedRAMP, HITRUST, MTCS, IRAP, and ENS. Technical details being shared with the government may be seen within the next few years.

4.6 Limitations and Considerations

It has been noted that these are newly discussed concepts, but it is anticipated that data localisation may be required for extremely sensitive data only and that this would constitute one of the limitations to an organisation collecting or transferring data in connection with foreign government data requests or foreign litigation proceedings. The Cloud Policy Framework (CPF) issued in June 2022 will set the road for more concrete considerations relating to the above-mentioned circumstances and operations.

4.7 "Blocking" Statutes

Pursuant to Article 15(3) of the QFC PDPL, 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.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

The virtuous cycle enabling AI revolution is composed of big data generated, computing power and algorithms. According to the National Artificial Intelligence strategy in Qatar, more than 94% of the Qatari population uses the internet.

AI methods tend to acquire "black box" characteristics. This context may lead to complete dismissal or ignorance of principles of fairness, accountability and transparency principles that are vital for data privacy. It is noted that AI algorithms will inherit any biases consecrated in data, and mechanisms are required that guarantee outputs which are consistent with the Qatari norms.

The profiling, microtargeting and online manipulation are all part of a bigger scheme where many technological companies are treating users and customers as end-products. As much as the principles of transparency, accountability and purposefulness are carved into the Qatari PDPL and guidelines, Qatar is yet to implement effective measures in practice to achieve its ambitions of cybersecurity protections and dealing with big data analytics, automated decision-making and AI sub-branches.

5.2 "Digital Governance" or Fair Data Practice Review Boards

The MOTC in the state of Qatar may in certain circumstances co-ordinate with any professional group or association, and any other association representing controllers or website operators for the purpose of self-organisation encouragement and development and raising awareness on PDPL and developing training and learning programmes. Digital governance is something yet to be examined in the Qatari jurisdiction.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation

According to Article 11(7) of the PDPL, data controllers are obliged to carry out comprehensive audits and reviews about the extent of their compliance with PDPL. Currently, nothing in the law provides for class action or collective redress.

According to the Guidelines, specifically related to data processors and data controllers, the contract must include obligations on the processor to assist the controller with audits and reviews of their compliance with the PDPL. Such obligations include:

- permitting the controller, or an auditor appointed by the controller, to audit compliance with its obligations under the PDPL;
- that the processor will contribute to such audits where required;
- which party will be financially responsible for such audits; and
- that the processor will make available all information as is required to show its compliance with the PDPL.

The auditor shall plan and perform a certification audit in two phases:

- Design Assessment – considered as preliminary assessment and verification that controls have been designed, documented, approved and communicated to relevant parties; and
- Operating Effectiveness Assessment – considered as final assessment.

5.4 Due Diligence

In corporate transactions, entities would need to gather information and assess the steps that should be taken into consideration to become compliant. The issues relevant to conducting diligence in corporate transactions would be met when assessing the gaps between different jurisdictions involved in the transaction, especially when reviewing cross-border provisions. The issues would be violation of non-disclosure provision or disclosure of unnecessary information during the due diligence.

5.5 Public Disclosure

According to the NCSA Guidelines, organisations must act relying on a base-risk approach. Currently, publicly traded companies are not obliged to disclose cybersecurity incidents and periodic disclosures about their cybersecurity policies and procedures. There is no provision in the PDPL providing for such obligation or disclosure duty, except for financial disclosure.

5.6 Digital Technology Regulation/ Convergence of Privacy, Competition and Consumer Protection Laws (Including AI)

The competition law and consumer protection law in Qatar converge on many aspects related to PDPL: specifically, for example, service providers shall ensure that customer information and customer communications are protected by security and technical safeguards that are appropriate to their sensitivity. It is prohibited under competition law to divulge any information or data relative to the implementation of the provisions of the Competition Act or to use the information for purposes other than those admitted under the law. Furthermore, according to telecoms law, the customer has the right to erasure and request that its information and personal data be erased.

5.7 Other Significant Issues

One of the key issues arising, relating to the implementation of PDPL and the constant innovations being witnessed in the digital field, is the use of social media platforms and the increasing impact these platforms are gaining in the Qatari jurisdiction as well as around the globe. The Qatari system's treatment of concurrent and fast developments in this area have yet to be seen. It is anticipated that many bilateral and multilateral agreements will be concluded with Qatar in the coming years regionally and internationally, specifically related to judicial assistance and cloud computing and deployment systems.

One of the significant challenges worth mentioning is that Qatar's national system will need to dive into the newly introduced systems related to AI and align with upcoming levels in order to ensure that there is development on a national scale in relation to this new digital tool. Discussions in the state of Qatar centre on the know-how and necessity of introducing a new legal framework and regulatory aspects related to the same.

The same applies to all sectors within the country that are still awaiting serious and impacting measures that could be implemented to cope with the AI industry and the AI tools recently being detected globally. One last issue being discussed is the disputes resolution scheme for disputes arising out of the AI industry and AI usage, particularly in the sector of data privacy: as of yet, no such work appears to have been done.

Trends and Developments

Contributed by:
Alex Saleh, Feras Gadamsi, Yousef Al Amly and Rana Moustafa
GLA & Company

GLA & Company is a regional MENA-based law firm with offices in Dubai, Abu Dhabi, Riyadh, Kuwait, Cairo and Beirut. It provides strategic, cost-effective and forward-thinking legal representation for companies seeking to do business in the Middle East. The firm boasts a diverse portfolio of clients, ranging from start-ups to global enterprises doing business in the Middle East. GLA's practice consists of a full-service law firm that handles everything from simple advisory work to complex contentious and non-contentious matters. With extensive experience advising clients in the key Gulf Cooperation Council (GCC) states of Kuwait, Saudi Arabia, Qatar and the United Arab Emirates (UAE) – as well as in Egypt and Lebanon – the firm offers unique insights for companies seeking quality legal services. Data protection and privacy, in particular, is a key focus area for the firm, considering the expansion and revamping of applicable laws and regulations across the GCC.

Authors

Alex Saleh is a founder and managing partner of GLA & Company and takes a leading regional role in the firm's M&A and private equity practice. With more than 25 years of experience in both the Gulf Cooperation Council and the USA, he has accumulated sizeable expertise in the areas of banking and finance, M&A, capital market deals and infrastructure projects. His experience garners praise from the leading legal directories and his transactions are regularly noted by the same institutions and organisations.

Feras Gadamsi is a partner based in the firm's Dubai office, leading GLA & Company's global technology, data and privacy practice. Feras also advises on compliance issues, including regional anti-bribery and anti-corruption laws, US FCPA, internal investigations, and audits. He started his career in private practice as an associate at Bracewell in Houston before moving to Dubai with King and Spalding. Immediately prior to joining the firm, Feras served as Regional General Counsel at IBM. He was formerly Uber's lawyer in the MEA region, serving as General Counsel for Middle East and Africa, Oracle Cerner's Regional General Counsel, and served as CLO and Head of Policy for a Dubai-based start-up.

Contributed by: Alex Saleh, Feras Gadamsi, Yousef Al Amly and Rana Moustafa, **GLA & Company**

Yousef Al Amly is a partner at GLA & Company, and is a dual-registered lawyer and certified practitioner in both the UK and Egypt. With accumulated years of experience in corporate, banking and finance, equity capital markets, and debt capital markets, Yousef has advised clients on complex corporate and commercial structures and transactions in relation to joint ventures, corporate restructuring, M&A, equity capital markets and commercial transactions (including franchise, distributorship and agency); and has advised high-profile companies in the Middle East on anti-money laundering means, cybersecurity and data protection. Yousef is a member of the UK Solicitors Regulatory Authority, the Egypt Bar Association, and the Egyptian Court of Appeals.

Rana Moustafa is an associate at GLA & Company with extensive experience in international and domestic commercial disputes. Rana's experience spans across the GCC and Europe, representing clients in Kuwait, Lebanon, Qatar, United Arab Emirates, Saudi Arabia, Egypt and France. She has experience in international and domestic arbitration, working on matters held under the auspices of ICC/DIFC-LCIA/CRCICA/DIAC/ICSID and CAS. Rana extended her experience in data protection while working on matters related to data protection disputes, data protection framework at the workplace and data protection policies for clients. She is a member of the Egypt Bar Association and is currently studying for the French Barreaux.

GLA & Company

Alex Saleh
Managing Partner

Tel: Kuwait +(965) 669 55516
UAE +(971) 54 997 4040
Email: alex.saleh@glaco.com
Web: www.glaco.com/attorneys/alex-saleh/

Introduction

This chapter of the guide explores some of the biggest trends and developments in Kuwait, from a partnership with one of the world's largest publicly traded companies designed to jump-start digital transformation across the country to the expanded adoption and deployment of artificial intelligence. In addition, there is examination of some of the laws and regulations that have been introduced this year to help support the country's wider goals under Kuwait Vision 2035.

Google Cloud – Kuwait Government Partnership

Kuwait is undergoing a digital transformation. At the forefront of this transformation is the strategic alliance between Google Cloud and the Kuwaiti government. The Google collaboration aligns well with Kuwait Vision 2035 ("Vision 2035"), a national development plan that envisions a dynamic, diversified and technologically advanced Kuwait that is nimble enough to adapt as technology is deployed in the country and even newer technologies are introduced over time. At its core, Vision 2035 seeks to reduce dependency on oil revenues by fostering economic diversification through the promotion of non-oil sectors.

The partnership between Google Cloud and the Kuwaiti government is designed to support the digitisation of government services, migration of national data securely to the cloud, and setting up a national digital skills programme. The decision to enter a public-private partnership with Google stems from the Kuwaiti government's commitment to enhance government efficiency through rapid digital transformation to stimulate economic growth across all sectors.

Initiated in January 2023, the collaboration marks a pivotal moment in Kuwait's journey towards a digital era, shaping not only its regulatory and governmental landscapes, but also changing the economic landscape. It also lays the foundation for tackling, and managing, the data trends anticipated to affect Kuwait's economy in the coming years.

Vision 2035 is also grounded in the values of fostering economic diversity, encouraging innovation, and embracing digital progress. These values all align with the nation's evolving trends and advancements in data protection and privacy regulations. As Kuwait embraces this digitised era, the alliance with Google Cloud becomes instrumental in steering the nation towards a future that makes Vision 2035 a reality.

Growing the non-oil sectors is essential to Vision 2035, so it should come as no surprise that technology is being used as a catalyst to power growth across all sectors. To do that, the proper infrastructure must be in place to support the deployment of cutting-edge technology. Being able to handle "big data" as datasets continue to grow, while simultaneously maintaining high levels of data security and privacy demanded by governments and individuals alike, is essential to empowering the type of economic growth Kuwait wants to see as part of Vision 2035.

Consequently, the establishment of data infrastructure capable of powering the type of growth projected in Kuwait becomes essential to fulfilling Vision 2035, and Kuwait's embrace of the potential of data-driven economies becomes a key part of realising Vision 2035. Kuwait's enactment of data privacy laws is also in line with Vision 2035, reflecting a commitment to fostering a technologically advanced society. These laws, modelled after their European and American counterparts, are intended to safeguard individuals' privacy, and create standards for the

utilisation of data. The regulations support the vision's broader goal of economic diversification and a digital ecosystem that supports projected growth under Vision 2035.

The strategic alliance between the Kuwaiti government and Google Cloud marks a significant milestone in Kuwait's journey towards digital transformation. The Kuwaiti government has allocated approximately KWD306 million for a seven-year implementation. The collaboration aims to leverage technologies in data analysis, cybersecurity, and AI, positioning Kuwait to keep up with the pace of technology globally and the expected economic growth under Vision 2035.

This partnership extends beyond technological advancements to encompass broader societal benefits. The collaboration focuses on healthcare, education, disaster management, and smart cities, all areas that are in line with Vision 2035. The agreement seeks to create new job opportunities for Kuwaiti youth by establishing a training programme targeting more than 5,000 citizens, students and workers. The partnership is a joint effort involving the Direct Investment Promotion Authority, the Central Agency for Information Technology, and the Communications and Information Technology Authority.

DPPR and effect of Google Cloud partnership

In 2021, Kuwait introduced Decision 42 of 2021 (the "Data Privacy and Protection Regulation", or DPPR), modelled after international data protection regulations like the General Data Protection Regulations (GDPR).

The DPPR serves as a more comprehensive framework than the preceding regulations. The DPPR is not a replacement but rather an addition to the Kuwait E-Transactions Law and the Data Classification policy. When it was first enacted, the DPPR originally addressed activities related, inter alia, to the storage, collection and processing of personal data, including sensitive personal data, performed in or out of Kuwait.

The DPPR has since evolved. Currently, the DPPR only applies to service providers engaged in the telecommunications sector and licensed by the Communication and Information Technology Regulatory Authority (CITRA).

The shift in DPPR's scope can be attributed to the collaboration between Google Cloud and the Kuwaiti government. The government changed the scope of the law because the law as originally drafted applied to all data collectors in Kuwait. However, with the introduction of the Google Cloud partnership, sensitive data that is required by law to be stored on the ground in Kuwait, would, in fact, be stored on the Google Cloud in the interim period, thus violating the law.

To address this challenge, the Kuwaiti government strategically carved out the DPPR to exclusively govern telecom providers initially. This temporary measure allows the government to ensure compliance within the telecom sector while creating a path to revert the regulations to their original form to encompass all data collectors.

Effects of the Kuwaiti government and Google partnership

The partnership encompasses an array of initiatives designed to digitise citizen services and elevate the efficiency of the government. Digitising citizen services ensures wider accessibility to the residents and citizens of Kuwait. Moreover, this digital transition is poised to streamline bureaucratic processes within the Kuwaiti government. By eliminating these hurdles, citizens

and residents can expect a more efficient and cohesive service experience.

Impact on businesses

Digitisation of services extends beyond the enhancement of resident experiences. It will also lead to a transformative shift for both local and foreign companies engaging in business activities in Kuwait. This new digital landscape will eventually streamline processes such as filing applications with the Competition Protection Authority or managing the closure of companies with multiple regulatory bodies.

Currently, not all of Kuwait's ministries have fully functioning online portals to submit applications or ask questions. Many applications and processes can only be completed or submitted using paper applications or even in-person visits to the different ministries in Kuwait. These changes would significantly impact the operations of foreign and local companies. It is expected that these changes could connect the systems of different regulatory bodies, which could lead to a full digitisation of processes, including acts that require interaction with different regulators.

Cybersecurity Regulations

Another notable trend in Kuwait is the government's heightened emphasis on data security and privacy regulations. Recognising the importance of safeguarding information, Kuwait is taking strides, with the help of its alliance with Google Cloud, to maintain all sensitive data in local data centres and draft relevant regulations to protect sensitive data.

This initiative aligns with a broader global movement of refining data protection standards and maintaining standard cybersecurity practices. This renewed focus on data security is evidenced by Kuwait's new cybersecurity regulations, including Decision No 7 of 2023 (General National Framework Regulation for the Classification of Electronic Data) and Decision No 35 of 2023 (National Framework for Cybersecurity Governance), which reiterate Kuwait's intention to establish a robust and comprehensive cybersecurity legal framework.

Additionally, the establishment of data centres, and the efficient management of data, also reinforce Kuwait's cybersecurity framework. This data-centric approach is in line with Vision 2035's overarching goal of ensuring national security and stability by safeguarding critical data assets.

Artificial Intelligence in Kuwait

Kuwait's digital revolution is also marked by significant strides in the deployment and adoption of artificial intelligence (AI) and other big data technologies. The intersection of these innovations is reshaping many of the nation's sectors including healthcare, education, finance, and government services.

Abundant data availability and a tech-savvy youth population drive AI and big data technology expansion in Kuwait. The government's focus on education and research plays a pivotal role in cultivating a skilled workforce for AI and data science. Initiatives from leading universities and research institutions are addressing the skills gap and fostering expertise in these domains.

While Kuwait envisions a promising future, challenges in its AI and big data journey include the need for a robust data infrastructure, concerns about data privacy and security, a shortage of skilled professionals, and regulatory and ethical considerations. Collaborative efforts among the government, industry, and academia are crucial to overcoming these challenges. As Kuwait

actively embraces AI applications in various sectors, from healthcare to finance, the demand for skilled professionals is only expected to rise.

Kuwait's alliance with Google Cloud acknowledges the importance of secure, robust and adaptable data centres in relation to the processing of even more data as technology is deployed to power economic growth, and it becomes even more important when factoring in the wider use and adoption of AI.

In alignment with Vision 2035, the expanded use, deployment and adoption of AI, together with the establishment of data centres in Kuwait, are transforming Kuwait's data landscape. Economically, the integration of advanced technologies is a major step in realising the government's goal of economic growth and a digitally driven society. An important aspect of Vision 2035 is the emphasis on economic diversification. The integration of AI technologies and the digitisation across all key sectors, especially non-oil and gas sectors, is aimed at driving innovation and efficiency, which will help Kuwait transition from its reliance on oil revenues to a more diversified economy.

In the realm of education, the digitisation of learning materials and the application of AI-driven education tools represent emerging data trends. This evolution also supports Vision 2035's goal of human capital development by leveraging data to enhance the quality of education and nurture a workforce equipped with digital skills.

Within Kuwait's healthcare sphere, a significant trend is the growing utilisation of data analytics coupled with AI. Kuwait's healthcare industry has already begun deploying AI on a limited basis, and it is expected that wider adoption of more AI-driven tools will help shape the present and future of medicine in Kuwait. The digitisation of health records and the application of AI in diagnostics contribute to more data-driven healthcare practices. The deployment of AI-driven technology in the healthcare sector will help build a healthier society through advanced and responsive healthcare services, which also aligns with the wider objectives of Vision 2035.

Conclusion

The collaborative efforts between Google Cloud and the Kuwaiti government have laid the groundwork for transformative data trends and developments in Kuwait. This partnership signifies a pivotal moment in Kuwait's journey towards a digital era, reshaping regulatory landscapes, governmental processes, and the overall economy.

Kuwait's heightened emphasis on data security and privacy, reinforced by new cybersecurity regulations introduced in 2023, reflects a commitment to establishing a comprehensive legal framework. The establishment of data centres and the efficient management of data underscore Kuwait's dedication to ensuring national security and stability by safeguarding critical data assets.

The impact of digitisation extends beyond regulatory and governmental spheres. Digitising citizen services enhances accessibility and streamlines bureaucratic processes, contributing to a more efficient and cohesive service experience for residents. For businesses, the shift towards digitisation of processes is poised to streamline operations, connecting the systems of different regulatory bodies, and impacting the way applications are filed.

Contributed by: Alex Saleh, Feras Gadamsi, Yousef Al Amly and Rana Moustafa, **GLA & Company**

In alignment with Vision 2035, the integration of AI and data centres stands as an important step towards realising the vision's goal of a digitally driven society. This extends into education, where the digitisation of learning materials and the application of AI-driven tools align with the vision's emphasis on human capital development. The healthcare sector experiences a significant trend with the growing utilisation of data analytics and AI, presenting a paradigm shift towards more data-driven healthcare practices.

As Kuwait continues forward into this new digitisation era, with the ongoing initiatives and implementations of Kuwait's evolving digital landscape, the alliance with Google Cloud contributes to the nation's digital transformation, supporting Vision 2035's aspirations for a diversified and advanced future.