Chambers AND PARTNERS

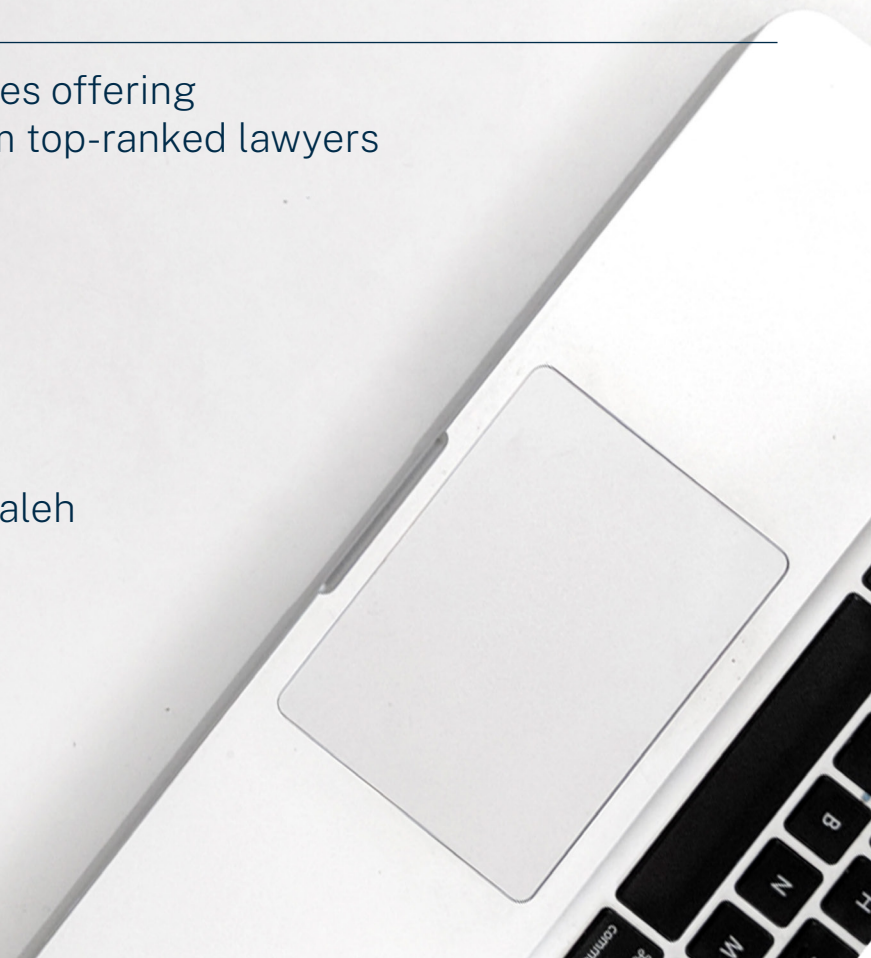
CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2025

Definitive global law guides offering comparative analysis from top-ranked lawyers

Quatar: Law & Practice

Alex Saleh, Asad Ahmad,
Dean Jaloudi and Jehan Saleh
GLA & Company



QATAR

Law and Practice

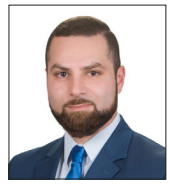
Contributed by:
Alex Saleh, Asad Ahmad, Dean Jaloudi and Jehan Saleh
GLA & Company

Contents

GLA & Company is a regional law firm based in the UAE, and 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. 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 in advising clients in the key Gulf Cooperation Council (GCC) states of Kuwait, Saudi Arabia, Qatar and the UAE – as well as in Egypt and Bahrain – the firm offers unique insights for companies seeking quality legal services. Data protection and privacy is an area of particular focus for the firm, considering the expansion and revamping of applicable laws and regulations across the GCC.

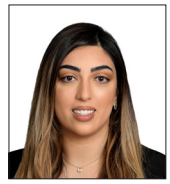
Authors

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.



Asad Ahmad is the legal director and head of the antitrust and competition practice at GLA & Company, and leads the firm's regional practice across Kuwait, Saudi Arabia, Qatar, the UAE, Egypt, and COMESA. He advises clients on merger control, competition compliance and regulatory matters, securing major clearances and handling high-profile investigations. Asad also leads GLA's data privacy team, guiding multinational clients on regulatory compliance and data protection strategies. A dedicated mentor and thought leader, he contributes to legal publications, conducts webinars and actively engages with competition regulators, reinforcing GLA's reputation as a leader in antitrust and competition law.

Dean Jaloudi is a partner and head of the Qatar office of GLA & Company. He has worked for international law firms in Doha since 2018, and previously worked as a corporate/commercial lawyer in Dubai from 2012 to 2017. Dean's area of expertise is equity capital markets (ECM) transactions on the Qatar Stock Exchange (QSE). He advised Baladna QPSC and QLM Life & Medical Insurance QPSC on their successful initial public offerings (IPOs) on the QSE. He also recently advised several Qatari companies on their proposed conversions and direct listings on the QSE.



Jehan Saleh is an associate attorney at GLA & Company. Her practice focuses primarily on corporate transactions and commercial advisory. A graduate of Wayne State Law School, Jehan previously clerked for a judge in the Wayne County Circuit Court in Michigan. Prior to joining GLA & Company, Jehan was an associate attorney for a medium-sized law firm in the United States, where she practised civil litigation. Jehan's Gulf experience includes working in the legal department for a large rideshare company in Dubai.

GLA & Company

Alex Saleh
Managing Partner

Tel: +965 669 55516
Email: alex.saleh@glaco.com
Web: www.glaco.com/attorneys/alex-saleh/

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Qatar introduced Qatari Law No 13 of 2016 (the "Personal Data Privacy Protection Law", or PDPPL), 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 PDPPL applies to personal data that is received, collected, extracted and/or processed through electronic or traditional methods. The PDPPL aligns with the universal data protection principles, which were established as the core of the European Union's General Data Protection Regulation (GDPR).

The Compliance and Data Protection Department (CDPD) attached to the Ministry of Communications and Information Technology (MCIT) (previously known as the Ministry of Transport and Communications (MOTC)) published guidelines concerning the PDPPL (the "Guidelines") in 2021, with the aim of providing a framework for data protection in Qatar.

The fundamental data protection provisions are aligned with:

- the Telecommunications Law promulgated by Decree Law No 34 of 2006;
- 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).

While these laws can supplement data protection and privacy laws in Qatar, the PDPPL is the detailed framework for the protection of personal data in Qatar.

In addition to the "mainland" or "State" system and the PDPPL described above, there is a separate legal data privacy protection regime in the Qatar Financial Centre (QFC). The QFC is a business and financial hub in Qatar that provides a legal, regulatory and tax environment distinct from "mainland Qatar". It operates under its own legal framework and has its own independent judiciary. The key data protection legislation for the QFC is the QFC Data Protection Regulations 2021 (the "QFC Regulations").

The Data Protection Office (DPO) is an independent institution of the QFC. It is charged with administrating the QFC Regulations and all aspects of data protection within the QFC.

1.2 Regulators

The CDPD at the MCIT is the key regulator in Qatar, and the National Cyber Security Agency (NCSA) is the competent department for administration and enforcement of the PDPPL. It is the key authority for conducting investigations regarding cybersecurity issues, implementing and examining issues related to national cyber-risks, and conducting fieldwork solidifying resil-

ience against cybercrimes and crises. All data breaches should be reported to the NCSA.

In the QFC, the DPO is concerned with the data protection framework. It is the institution charged with providing guidance on all data protection matters or complaints related to the QFC 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 Enforcement Proceedings and Fines

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

The competent department, as listed in the PDPPL, will issue a rectification decision, ordering the violating entity to rectify the violation within a fixed period, as per Article 26 of the PDPPL. Previously it was understood that the competent department was the MCIT; however, recently the NCSA clarified that this department was not yet designated. The controller or processor has the right to file a "grievance" against such order to the relevant 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 PDPPL. According to Article 29 of the PDPPL, the judicial officers and/or law enforcement officers designated by the NCSA have the power to seize and document any crimes related to violations of the provisions of the law.

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

- to act or omit from performing 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 Data Protection Fines in Practice

Increasing activity has been seen by the regulators in both the State of Qatar and the QFC; however, no more than a handful of publicly announced fines or actions have occurred, and the NCSA and QFC have not disclosed the names of the offending companies.

1.5 AI Regulation

The NCSA recently issued the Guidelines for Secure Adoption and Usage of Artificial Intelligence. This publication aims to provide guidance to organisations on how to securely deploy AI systems and products. The guidelines address critical risks such as privacy violations, AI bias, security vulnerabilities and compliance challenges, particularly in sectors where AI processes personal data (such as finance, healthcare and law enforcement). Safeguards include role-based access controls and strong encryption to secure AI data processing.

Further, AI systems must comply with PDPPL requirements for data minimisation, purpose limitation and lawful processing. AI models must incorporate auditability, traceability and documentation requirements. Additionally, organisations must adopt adaptive risk management frameworks and human-in-the-loop mecha-

nisms to supervise AI-driven decision-making and mitigate bias.

Additionally, the QCB recently issued guidelines to ensure the ethical use of AI in the financial sector. These guidelines mirror the PDPPL safeguards by stating that AI systems must only collect and process personal data necessary for their intended function, and must not be used beyond the defined purpose. Financial institutions must provide clear explanations to users about how their data is processed by AI systems. Customers should be informed if AI-driven decisions affect them, and about the reasoning behind the decisions.

AI-driven systems must obtain explicit consent from individuals before processing their data.

1.6 Interplay Between AI and Data Protection Regulations

As previously mentioned, all AI guidelines in Qatar are closely tied to the PDPPL, ensuring that AI systems handling personal data comply with national privacy laws. AI deployers must ensure that AI models only process data for lawful and predefined purposes, in line with the PDPPL's consent and data minimisation principles.

2. Privacy Litigation

2.1 General Overview

Requirement to Appoint Privacy Protection Officers

The PDPPL does not provide for an express obligation on organisations in Qatar or the QFC to appoint a data protection officer. Nevertheless, there is an obligation on the data controller to specify processors responsible for protecting personal data, to train them appropriately on the protection of personal data and to 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 PDPPL. 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; specifically, describing 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 PDPPL.

An individual may, at any time, have access to their personal data and request its review, in the presence 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 as mentioned above, no person may request access to any personal information held by an authority, other than their personal data.

As recently discussed, a practical example explaining the criteria necessary for collection and processing is the collection and tracking of

points of players, their movements and positioning during the FIFA World Cup 2022. According to the PDPPL, this is considered processing. However, even if the GDPR and the PDPPL require prior express consent, an examination has concluded that, in the context of the FIFA World Cup, the players impliedly consented to the processing of such personal data by the World Cup organisers.

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

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

The PDPPL 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 into 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, the Data Protection Impact Assessment (DPIA) and a Record of Personal Data Processing are key components of any personal data management system. This aligns with the provisions in Articles 13 and 11(1) of the PDPPL.

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

Implementation of Internal/External Policies and Data Subject Rights

According to the PDPPL 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

In the State of Qatar, the PDPPL provides 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 DPIA before undertaking any processing activities. This would be applicable in 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, Article 3 of the PDPPL provides that data processing must be in conformity with the law and principles of good faith. A request permit from the CDPD at the MCIT should be submitted and 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 CDPD. In the same vein, data controllers will need to submit the relevant DPIA and any other additional information that the CDPD may request. Currently, such documents are submitted by email. However, an online portal that would facilitate such submissions is expected to be launched soon.

Definition of Harm to National Privacy and Data Protection Under the PDPPL

A personal data breach means a breach of security leading to the unlawful or accidental alteration, destruction, loss, or 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 impacts being suffered by individuals, organisations and/or communities, such as:

- compromised personal safety or privacy;
- the burden of additional legal obligations or regulatory penalties;
- 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.

Sensitive or Special Data

In the State of Qatar, the PDPPL addresses the concept of sensitive personal data, first introduced in the EU in its framework on data protection and human rights. The PDPPL specifically defines sensitive date as any data consisting of information as to a natural person's:

- ethnic origin/race;
- 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 MCIT.

The PDPPL 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 to biometric and genetic data.

The QFC Regulations further stipulate that there must be a particular and specific permit for the processing of sensitive data. Article 12 of the Regulations states 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 to disclose 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 in place by the data controller, to ensure the security of the sensitive personal data.

Special Overview of Children's Websites

The PDPPL 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, in practice this is widely viewed as engulfing various categories of digital media, including social media applications.

Internet and Online Streaming

Moreover, as regards the internet and online streaming, the PDPPL as well as 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, any other political or governmental figure, or any religious figure.

Specific Overview of the Banking Sector

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

- raising awareness internally and among their service providers;
- conducting due process and reviewing internal policies, disclaimers, consents or agreements, and ensuring their compliance with the PDPPL;
- 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 made to protect customer data.

Specific Overview of the QFC

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

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

Specific Overview of the Health Sector and Private Health Data

Under Article 16 of the PDPPL, private health data includes personal information related to:

- an ethnic group;
- children;
- a 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 must first be obtained explicitly or by confirmation.

2.2 Recent Case Law

As of January 2025, Qatar has no reported significant case law or ongoing litigation specifically concerning data protection or AI comparable with the jurisprudence of the Court of Justice of the European Union (CJEU) regarding Articles 82 and 83 of the GDPR. However, there have been recent regulatory developments, including the introduction of new AI guidelines.

2.3 Collective Redress Mechanisms

Collective redress mechanisms are not outlined under the PDPPL. However, the PDPPL does provide a complaint and enforcement mechanism that allows individuals to seek redress for data protection issues. Article 26 grants individuals the right to file complaints with the competent department if they believe their personal data has been processed unlawfully. Such department will then investigate, and can issue binding corrective decisions to rectify breaches. If a violation is confirmed, the competent department may order the data controller or processor to correct the breach within a specified timeframe.

If the controller fails to comply, further regulatory actions may be taken.

While the PDPPL does not outline a class action process, individuals retain the right to pursue civil claims in Qatari courts for damages resulting from data breaches. Articles 23–25 impose fines of up to QAR5 million for non-compliance with specific PDPPL provisions, reinforcing the financial accountability of data controllers and processors.

3. Data Regulation on IoT Providers, Data Holders and Data Processing Services

3.1 Objectives and Scope of Data Regulation

The authors are not aware of any legislation in Qatar with respect to IOT services.

3.2 Interaction of Data Regulation and Data Protection

The PDPPL is closely linked to other Qatari laws regulating cybersecurity and digital transactions. The NCSA enforces cybersecurity laws and plays a role in ensuring personal data protection in AI applications and IOT services. The Telecommunications Law and Cybercrime Law

impose additional restrictions on electronic data processing and cybersecurity threats.

3.3 Rights and Obligations Under Applicable Data Regulation

The authors are not aware of any legislation in Qatar with respect to IOT services.

3.4 Regulators and Enforcement

See **1.2 Regulators**.

4. Sectoral Issues

4.1 Use of Cookies

According to the Guidelines, controllers may use "cookies" on an individual's web browser to target direct advertisement 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.

4.2 Personalised Advertising and Other Online Marketing Practices

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

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

- 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.

4.3 Employment Privacy Law

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.

According to the PDPPL, workplace privacy rules strictly provide for a solid framework for protecting an 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 CDPD.

On 24 May 2021, the Ministry of Administrative Development, Labour and Social Affairs (MADLSA) launched the first phase of the Unified Platform for Complaints and 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 against entities with business regulated by the MADLSA.

4.4 Transfer of Personal Data in Asset Deals

The PDPPL does not contain explicit provisions regarding data transfers during M&A or asset deals. However, data controllers must comply with the core principles of consent and lawful processing, ensuring that personal data is transferred in line with the PDPPL's transparency and data minimisation requirements.

5. International Considerations

5.1 Restrictions on International Data Transfers

Trans-border data flow is defined under the PDPPL as accessing, viewing, retrieving, using or storing personal data without border constraints. The PDPPL provides that data controllers should not take measures or adopt procedures that may restrict or prevent trans-border data flow, unless processing such data violates the provisions of the PDPPL or will cause gross damage to the data subject.

More specifically, the law reserves the right for governmental bodies to determine that this principle, among 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.

A trans-border 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 countries where the data is stored.

5.2 Government Notifications and Approvals

Situations 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, the 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, this 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 Regulations.

5.3 Data Localisation Requirements

From an operational perspective, according to the Communications Regulatory Authority (Qatar's telecommunications and digital services

regulator), 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.

The Cloud Policy Framework (CPF) issued in June 2022 sets the roadmap for more concrete considerations relating to the above-mentioned circumstances and operations. According to the CPF, data residency shall no longer be a requirement as data classification schemes, security and encryption technologies now secure a high level of protection controls.

It has been noted that these are newly discussed concepts, but it is expected 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.

5.4 Blocking Statutes

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

5.5 Recent Developments

There have been no recent developments in the regulation of the international transfer of personal data. However, given that neighbouring countries have enacted amendments to supplement their own data protection laws, Qatar may follow suit by introducing updates to its PDPPL to align with regional and global standards.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com