



QATAR

Data Protection Laws of the World

Introduction



Welcome to the 15th update of the Data Protection Laws of the World handbook. Data protection and privacy laws continue to evolve at pace, reflecting responses to technological change, increasing data-driven business models and heightened expectations around accountability and enforcement. Alongside jurisdiction-specific reform, a number of clear global trends are emerging, including increasing enforcement action, greater data localization and complexities with data transfers, and closer alignment between data protection, cybersecurity and wider digital regulation, all set within a backdrop of heightened geopolitical tensions. As a result, keeping track of developments across jurisdictions has become both more important and more challenging for organisations operating internationally.

Recent legislative and enforcement developments

This edition reflects another busy year for privacy and data protection, with new legislation taking effect in key markets such as India, while enforcement of established data protection laws, such as those in Europe, continues to be influenced by an increasingly complex geopolitical environment and escalating cyber threats.

Developments in the United States

In the United States, consumer privacy laws continue to rapidly develop at the state level, with the passage of more than 20 state comprehensive consumer privacy laws and increased state and multi-state enforcement. Recently, minor privacy laws have been passed and taken effect in a number of states, imposing privacy obligations and restrictions on websites and online services that provide services that are directed at minors under 18 years old or that collect personal information about known minors under 18 years old. In addition to increased regulator enforcement, privacy litigation is on the rise in the United States – key areas of focus for privacy litigation and class action risk include minor privacy and safety, online tracking, data breaches and cyber incidents, text marketing, and biometrics.

Responding to a rapidly evolving landscape

To support clients in navigating this fast-moving landscape, Data Protection Laws of the World will now be updated twice per year, reflecting the accelerating pace of reform within the data protection and privacy landscape and the growing need for up-to-date, practical insight.



Data protection laws

Note: Please also see [Qatar Financial Center](#) (a business center located on-shore in Qatar with its own regulations separate from those of the State of Qatar, including separate data protection regulations).

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

Qatar has implemented Law No. (13) of 2016 Concerning Personal Data Protection ("the **Data Protection Law**").

With its Data Protection Law – adopted in 2016 – Qatar became the first Gulf Cooperation Council (GCC) member state to issue a generally applicable data protection law.

The Data Protection Law is supplemented with a set of regulatory guidelines issued by the National Cyber Governance and Assurance Affairs (NCGAA) of the National Cyber Security Agency. The guidelines incorporate concepts from EU privacy regulatory frameworks and seek to clarify obligations under, and address matters that are not dealt with in, the Data Protection Law. The introduction of these guidelines provide a mechanism for which those subject to the Data Protection Law would be able to better understand their obligations under the Data Protection Law and comply with its provisions more fully.

The Data Protection Law applies to personal data when this data is any of the following:

- Processed electronically;
- Obtained, collected or extracted in any other way in preparation for electronic processing; and
- Processed by combining electronic processing and traditional processing.

The Data Protection Law provides that each individual shall have the right to privacy of their personal data. Such data may only be processed within a framework of transparency, honesty, respect for human dignity and in accordance with the provisions of the Data Protection Law.

Definitions

Definition of personal data

Personal data is defined under the Data Protection Law as data relating to a natural person whose identity is identified or is reasonably identifiable, whether through this data or by means of combining this data with any other data or details.

Definition of sensitive personal data

Sensitive personal data means personal data consisting of information as to a natural person's:

- Ethnic origin
- Health
- Physical or mental health or condition
- Religious beliefs
- Relationships
- Criminal records

National data protection authority

National Cyber Governance and Assurance Affairs (NCGAA) of the National Cyber Security Agency

Registration

There is currently no requirement in Qatar for data controllers who process personal information to register with the regulator, the NCGAA.

Data protection officers

There is currently no obligation for organizations in Qatar to appoint a data protection officer. 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.

Collection and processing

Generally, data subject consent is required to collect and process personal data, except to the extent processing is deemed necessary for a lawful purpose of the controller, or the third party to whom the personal data is sent.

Lawful purpose is defined in the Data Protection Law as "the purpose for which the personal data of the data subject is being processed in accordance with the law," which includes cases where a data controller is processing personal data for legitimate interests and specific purposes set forth under Data Protection Law as described below.

Prior to processing personal data, the data controller must notify the data subject of the following information:

- The details of the data controller or another party who processes the data on behalf of the data controller;
- The lawful purpose for which the data controller or any third party wants to process the personal data;
- A comprehensive and accurate description of the processing activities and the degrees of disclosure of personal data for the lawful purpose; and
- Any other information deemed necessary and required for the satisfaction of personal data processing.

The data controller is free to process data without the consent of the data subject or a lawful purpose in the following circumstances:

- The data processing is in the public interest. A data controller would process personal data in the public interest if it is conducting a specific task in the public interest pursuant to applicable law or is exercising "official authority" (e.g. a public body's tasks, functions or duties) pursuant to applicable law;
- The data processing is required to meet a legal obligation. A data controller would be considered processing personal data to meet a legal obligation where it is required to do so by virtue of the law or court order;
- The data processing is required to protect the data subject's vital interests. What constitutes as "vital interests" is applied very narrowly to cases of "life and death" and on the basis of humanitarian grounds such as in relation to a pandemic / epidemic. Further, this exemption is likely to arise in cases where data related health is being processed which is a category of sensitive personal data (explored further below) and in which case, this exemption would only apply if the data subject is physically or legally incapable of providing consent and as such, explicit consent may be more appropriate in the circumstances;
- The data processing is required for scientific research being conducted in the public interest. Cases involving the processing of personal data for "scientific research in the public interests" should be interpreted broadly and would include processing activities to further technological development or privately funded research; or
- The data processing is required to investigate a crime, if officially requested by the investigating authorities.

Sensitive personal data may not be processed except after obtaining authorization from the NCGAA. There is a high threshold for processing this data and, amongst other things, a data controller would be required to:

- Identify a permitted reason for processing sensitive personal data and an "additional condition" for processing activities and these "additional conditions" include, but are not limited to, (i) processing with the data subject's explicit consent or parental consent (as may be relevant), (ii) the personal data is made public by the data subject; or (iii) the processing is necessary in an employment context and would enable the data controller to fulfil their obligations as an employer;
- Complete a data protection impact assessment to identify, inter alia, the purpose and permitted reason for processing, the potential damage / harm that can be caused to the data subject as a result of the processing activities and the risks to the processing and methods / actions to mitigate such risks; and
- Obtain permission from the NCGAA to process such personal data which may be conditioned on, inter alia, the data controller evidencing to the NCGAA that it has the appropriate administrative, technical and financial precautions in place to protect such special personal data.

Transfer of personal data

Data controllers may collect, process and transfer personal data when the data subject consents, unless deemed necessary for realizing a 'lawful purpose' for the controller or for the third party to whom the personal data is sent. The data controller has to demonstrate, when disclosing and transferring personal data to the data processor, that the transfer is for a lawful purpose and that the transfer of data is made pursuant to the provisions of the Data Protection Law.

Data controllers should not take measures or adopt procedures that may curb trans-border data flow, unless processing such data violates the provisions of the Data Protection Law or will cause gross damage to the data subject. The Data Protection Law defines 'trans-border data flow' as accessing, viewing, retrieving, using or storing personal data without the constraints of state borders.

Security

Data controllers must take appropriate technical and organizational measures to securely manage personal data.

The data controller must carry out the following procedures:

- Review privacy protection procedures before implementing new processing operations
- Specify the processors responsible for protecting the personal data
- Train processors on the protection of personal data and raise their awareness relating to the same

- Set up internal systems to receive and investigate complaints, data access requests, data correction or deletion requests and provide the data subjects with information relating to the same
- Set up internal systems for the effective management of personal data, and report any violation of the same with the aim of safeguarding personal data
- Adopt suitable technical means to enable individuals to exercise their rights to access, review and correct their personal data directly
- Carry out comprehensive review and checking of the commitment to protect personal data
- Verify that the data processor abides by the instructions given to him/her or take suitable precautions to protect personal data, and continually monitor that situation

The data controller and processor must take necessary precautions to protect personal data against loss, damage, amendment, disclosure or access thereto or use thereof in an accidental or unlawful way. The Data Protection Law states the precautions taken must be proportionate to the nature and importance of the personal data to be protected. Organizations should adopt best practice methodologies in keeping with their business sector.

Breach notification

There is an obligation on the data controller to notify the regulator, the NCGAA and the data subject of any breaches of the measures to protect the data subject's privacy if it is likely to cause damage to the data subject. The notification to the NCGAA and the data subject must be made as soon as possible from the time the data controller becomes aware of the breach but in any event, within 72 hours.

A personal data breach means a breach of security leading to an unlawful or accidental alteration, destruction, loss, unauthorised disclosure of, or access to personal data. This would encompass both, accidental and deliberate breaches such as, theft or loss of IT equipment, inadequate disposal of confidential files that may contain personal data material and using client data for a personal gain. In assessing whether a breach would cause serious damage, the data controller should take into consideration whether the breach would cause the data subject to be impacted negatively in various ways such as emotional distress, or physical or material damage.

Enforcement

In Qatar, the NCGAA is responsible for the enforcement of the Data Protection Law. Any data subject may submit a complaint to the NCGAA in the case of a violation of the Data Protection Law. The NCGAA will investigate the complaint and, if the complaint is found to be valid, the NCGAA can oblige the data controller or processor to rectify the violation within a specified time period.

The NCGAA can also impose fines of up to 5 million (US\$1.4 million) for violations of the Data Protection Law.

Electronic marketing

Unsolicited direct marketing is prohibited under the Data Protection Law, which requires prior consent to send electronic marketing communications (including by wired or wireless communication). The consent of the data subject must be affirmative, explicit and unambiguous. Indirect or implied consent by means of pre-ticked boxes may be deemed invalid.

All electronic marketing communications must include the identity of the sender and an indication that it is sent for the purpose of direct marketing. The message must include an address that can easily be reached and must enable the recipient to send a message requesting the sender to stop the electronic communication and enable the recipient to withdraw the consent at any time.

Online privacy

The Data Protection Law specifically regulates online privacy processing data in relation to children. Owners and operators of websites must observe the followings requirements.

In relation to online privacy, data controllers must ensure they have in place a privacy notice to notify data subjects that they are processing personal data. A privacy notice must generally include the following information:

- Details of the data controller including its legal name, registered address and contact information
- Details regarding third-party processors if any and in which case, the privacy notice should, inter alia, provide a description of why the data processors are processing information on behalf of the data controller
- The data controller's purposes for processing personal data including the permitted reasons for doing so
- A comprehensive and accurate description of the processing activities
- The levels of disclosure for the permitted reasons for processing personal data or a general description
- Any other information that is necessary for fulfilling conditions of personal data processing for e.g., general information on how personal data is kept secure and a data subject's rights and how they may be exercised

In relation to websites relating to children, a data controller should:

- Place a notification on the website regarding how children's data is used and its disclosure policies
- Obtain express approval from the parents or guardian of the child before processing any personal data
- Provide the child's parent or guardian—upon request and after verifying the identity of the child's parent or guardian—a description of the personal data that is being processed, stating the purpose of the processing, and a copy of the child's data that is being collected and processed

- Delete, erase, or suspend the processing of any personal data that was collected from the child or about the child, if the child's parent or guardian requests this, and
- Refrain from making any child's participation in a game or prize offer, or any other activity conditional on the child's submission of personal data which goes beyond what is required for the purposes of participation in the game or prize offer

Data protection lawyers



Brenda Hill

Legal Director

DLA Piper

brenda.hill@dlapiper.com

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:



Carolyn Bigg

Partner
Global Co-Chair Data, Privacy and
Cybersecurity Group
carolyn.bigg@dlapiper.com
[Full bio](#)



John Magee

Partner
Global Co-Chair Data, Privacy and
Cybersecurity Group
john.magee@dlapiper.com
[Full bio](#)



Andrew Serwin

Partner
Global Co-Chair Data, Privacy and
Cybersecurity Group
andrew.serwin@us.dlapiper.com
[Full bio](#)

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com