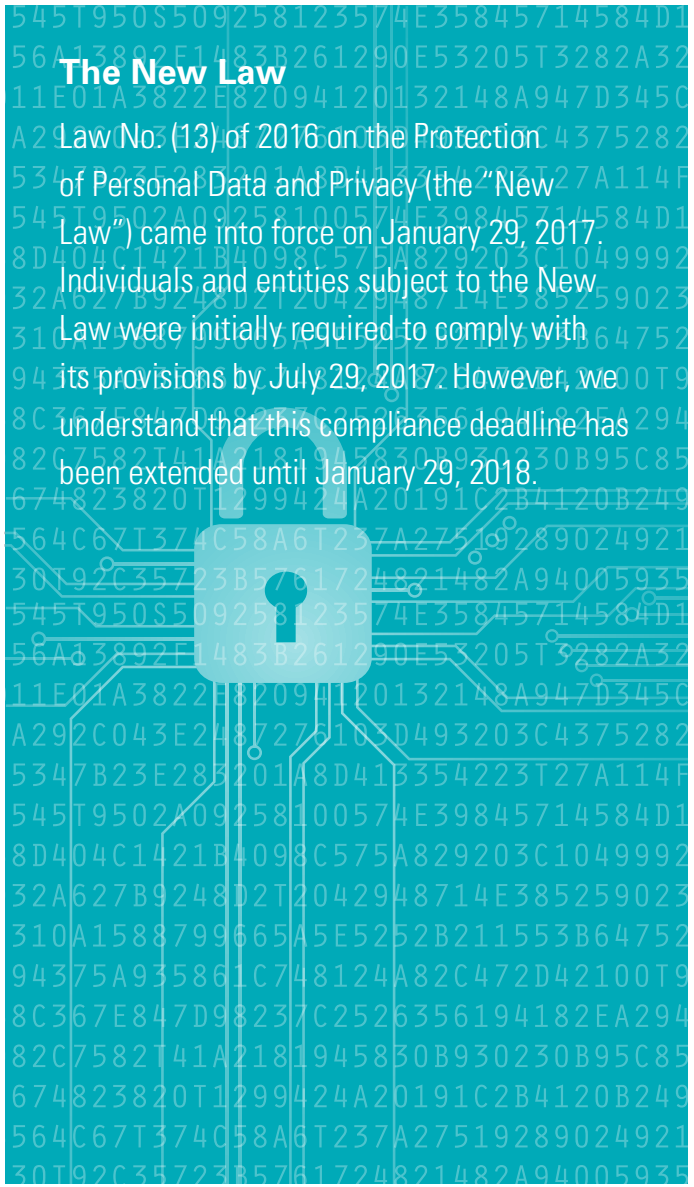
SQUIRE PATTON BOGGS

Qatar's New Protection of Personal Data Privacy Law

The New Law

Law No. (13) of 2016 on the Protection of Personal Data and Privacy (the "New Law") came into force on January 29, 2017. Individuals and entities subject to the New Law were initially required to comply with its provisions by July 29, 2017. However, we understand that this compliance deadline has been extended until January 29, 2018.



Who is Covered?

The New Law imposes obligations on any individual or entity collecting and electronically processing personal data. "Personal data" is defined broadly as "any information relating to an individual identified or reasonably identifiable by reference to such information or by combining such information with any other information." As such, the New Law impacts employers, healthcare providers, universities and B2C entities, along with any entity or individual supporting them in the collection and/or processing of personal data. Those supplying cloud or other remote data processing services are also covered under the law.

What is the Risk?

Failure to follow the New Law can lead to fines of up to QR5 million (US$1.3 million). To the extent of its violation, any contract or agreement concluded in violation of the New Law shall be considered null and void.

New Categories

The New Law creates the categories of "controllers," defined as the entity who "determines the means and purposes of processing personal data" and "processors," defined as the entity who "processes personal data on behalf of a controller."

Why Choose Us

Ranked as a top 10 global firm for many years, we have the wealth of resources and knowledge focused on creating a data privacy and cybersecurity compliance program that works for your company across the globe. In Europe, we have a large EU Data Privacy & Cybersecurity team located in key countries, including Belgium, Germany, France and the UK. We also have experts in North America, counseling companies on the cutting edge of the latest technologies facing cybersecurity and data privacy issues. Our team in the Middle East and Asia Pacific is experienced and has resources spread throughout the region in critical countries. Wherever your need, we can help you navigate your data privacy and cybersecurity legal needs, resulting in a coherent policy across your organization.

The types of data privacy and cybersecurity projects we can assist globally include:

- EU General Data Protection Regulations compliance
- Privacy Impact Assessments
- Strategic policy, legal and regulatory support
- Cybersecurity preparedness and crisis management
- Website compliance
- Compliance issues in cross-border investigations
- Whistleblower hotlines
- International data transfer compliance
- New product compliance, including Internet of Things (IoT)
- Data breach
- Privacy and cybersecurity litigation

Key Provisions

The New Law has several provisions that will have a far-reaching effect on how a company collects, processes and stores personal data.

- **Individual Rights** – The New Law establishes the right of an individual to privacy over his or her personal data. The individual is granted rights to:
  - Review, alter or delete their personal data at any time. An individual may request a copy of their personal data after making a payment that does not exceed the value of the service provided.
  - Withdraw approval at any time.
  - Object to the processing of their personal data, if it is unnecessary for the purposes for which it was given or is discriminatory.
- **Controller Duties** – A controller must do the following:

  Notification/Communication Requirements:
  - Obtain the approval of the individual before processing their personal data, unless they can show it is necessary to achieve the controller's (or the 3rd party to whom the personal data is sent) legitimate purpose.
  - Obtain explicit consent from the parent before processing any personal data of a child.
  - Obtain approval of the Ministry of Transport and Communications (MTC) before processing any "personal data of a special nature," which includes ethnic origin, health, physical/psychological state, religious beliefs, marital relationships and criminal offenses.
  - Notify the individual before processing (or allowing a 3rd party to process) personal data. This notice shall include the legitimate purposes for the processing, a description of the processing activities and the degrees of disclosure to be made.
  - Conduct direct marketing only after approval of the individual, which can be withdrawn, and must include the identity/address of the sender. (See also the Anti-Spam regulations issued by the Communications Regulatory Authority in November 2017).
  - Notify the individual and the government of any breach of personal data that would result in serious damage to the privacy of the individual.
  - Notify the individual of a disclosure of any inaccurate personal data.

  Implement Data Privacy Protection Procedures:
  - Take "necessary and appropriate precautions" to protect personal data from incidental or illegitimate loss, damage, modification, disclosure, access or use. This includes complying with privacy protection policies issued by the government.
  - Train, educate and conduct comprehensive security reviews on any staff or 3rd party processors handling personal data.
  - Delete personal data after it is no longer needed to achieve the legitimate purposes.
  - Implement a system to effectively manage personal data breaches.
  - Make available a method to receive and handle an individual's complaints, data access, correction or deletion requests.

Note: Trans-border data flows are encouraged, but must only be done in compliance of the New Law. Also, there is a broad carve-out to following the above rules when processing data for government or other civic purposes.

- **Processor Duties** – In addition to the items applicable above, the processor must:
  - Notify the controller immediately after it becomes aware of a breach or threat.
  - Take necessary and appropriate precautions to protect personal data from incidental or illegitimate loss, damage, modification, disclosure, access or use.
- **Complaint Process** – An individual may lodge a complaint with the MTC's privacy department, who will render a decision and, as needed, require corrective action. That decision may be appealed within 60 days. MTC's minister will have 60 days to either grant the appeal, or failing response, the decision is determined final.

What to Do

It is important for companies to prepare for the New Law to able to comply with many of the new provisions. Below is an overview of some of the projects that we can work with your team to implement.

- **Preliminary Due Diligence** – Start gathering information and assessing what steps your organization needs to take to become compliant. We can provide a gap assessment to identify what obligations you are under, whether in Qatar, Europe or elsewhere. Many countries are passing new data privacy laws which are applying to data held cross-border.
- **Data Mapping** – You can only protect what you know you have. Review and map your internal and external data flows and ensure appropriate privacy mechanisms are in place.
- **Consent-Based Data Uses, Special Data Processing** – The New Law requires valid consent and, in some cases, contains additional obligations/authorization from the government before processing personal data of a special nature. All processing activities should be reviewed and made to conform with the regulation.
- **Privacy Notices and Consents** – In order to ensure proper consent is obtained, privacy notices, consent forms and processes should be reviewed and amended accordingly.
- **Individuals Rights** – The New Law introduces new rights for individuals. Organizations must put in place procedures allowing individuals to effectively exercise their rights.
- **Privacy by Design** – Compliance with the New Law requires precautions be built-in to products and systems to protect individual's personal data. Procedures should be reviewed and amended, if existing, or developed and formalized, as necessary.
- **International Data Transfers** – Trans-border data flows may only be carried out in compliance with the New Law. Processor agreements and controller-to-controller agreements/clauses should be reviewed and updated.
- **Data Security Management Process** – Organizations must take appropriate technical and organizational data security measures, including comprehensive security reviews, training and testing/auditing of anyone handling Personal Data (including 3rd parties). It is important that businesses understand the required security measures and, if necessary, modify their breach management process to become compliant.
- **Breach Notification**: The New Law requires the reporting of data breaches to the individual and supervisory authority. Businesses must implement an appropriate breach notification plan.

Contact

Scott Warren
Partner, Tokyo
T +81 3 5774 1800
E scott.warren@squirepb.com

Charbel Maakaron
Managing Partner, Doha
T +974 4453 2500
E charbel.maakaron@squirepb.com