The New Qatar National Privacy Law: First of its Kind in the GCC

Presenter: Kelly Tymburski

4 March 2017

DISCLOSURE STATEMENT

DENTONS

Speaker:

Kelly Tymburski, LLB

- Has disclosed financial relationships but due to confidentiality cannot disclose Pharmaceutical companies names.
- Will not be discussing any unlabeled/unapproved use of drugs or products

Weill Cornell Medicine-Qatar

Overview

1. Background and the Existing State of the Law in Qatar on Privacy
2. Setting the Scene
   - Key data protection / privacy terminology and principles – an international perspective
3. New National Privacy Law – Application and Key Features
   - What is "personal data" and "sensitive personal data"?
   - What are the core principles under which data can be processed?
   - Consent requirements
   - Exemptions from the Law
   - Cross border transfers of information
   - Electronic communications for direct marketing
   - Enforcement & penalties
4. Compliance - What to do Next?
   - Coming into force – grace period
   - Your compliance "to-do list"

Background and Existing State of the Law in Qatar on Privacy

- Privacy rights and obligations appear across various laws
- Qatari Constitution - a general right of privacy for individuals
  - "*the sanctity of human privacy shall be inviolable, and therefore interference into privacy of a person, family affairs, home of residence, correspondence, or any other act of interference that may demean or defame a person may not be allowed save as limited by the provisions of the law stipulated therein.*"
- Qatar Penal Code
  - prohibits dissemination of news, photos or information "*related to secrets of private life, or families, or individuals*" – even if the information is true
- Cybercrime Prevention Law
  - Various clauses that criminalize unauthorized access, use or interception of information using electronic means
- Many such laws are also sector specific
  - Electronic Commerce and Transactions Law
  - Telecommunications Law

Background and Existing State of the Law in Qatar on Privacy (Cont'd)

- Qatar Financial Centre
  - QFC Data Protection Regulations
  - QFC Data Protection Rules
- Modeled on EU Directive 95/46/EC
- QFC law 7 of 2005: *'the QFC Laws and Regulations shall apply to The Contracts, Transactions and arrangements conducted by the entities established in, or operating from The QFC, with parties or Entities located in The QFC or in the State but outside The QFC, unless the parties agree otherwise.'*
- Under the QFC DP regime – all data must be:

  (i) processed fairly, lawfully and securely;

  (ii) 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;

  (iii) adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed;

  (iv) accurate and, where necessary, kept up to date; and

  (v) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data was collected or for which they are further processed.
- Further obligations are also imposed relating to security, data subject rights, controls on transfers outside of QFC - largely in line with wider EU Directive position

Setting the Scene – Understanding Key DP Terminology & Principles

https://www.youtube.com/watch?v=vHvd6HaPq_s

New National Privacy Law – Application and Key Features

New National Privacy Law – Application and Key Features

In the slides that follow, we will discuss each of the following key aspects of the new Law:

- What is "personal data" and "sensitive personal data"?
- What are the core principles under which data can be processed?
- Consent requirements
- Exemptions from the Law
- Cross border transfers of information
- Electronic communications for direct marketing
- Enforcement & penalties

"Personal Data" and "Sensitive Personal Data"

Personal Data:

"Information about an individual who has a verified identity, or can be verified reasonably; whether through such information or by combining between such information and other data."

Sensitive Personal Data:

"Personal data shall be deemed sensitive if related to the ethnic origin, children, ***health****,* ***physical or psychological condition****, religion, marital relations or criminal actions."*

Core Principles for Data Processing

- Personal data of an individual is to be processed in accordance with certain principles under the Law, including those of:
  - transparency
  - integrity
  - respect for human dignity
  - acceptable practices
- The Law applies whether processing occurs by electronic or non-electronic means
- Information disclosure obligations - i.e. must inform data subjects of:
  - purposes for collection
  - parties to be involved in processing activities
  - manner of processing
- Data controllers must **limit** their collection and retention of personal data to that which is **relevant** and **necessary** to achieve the **purposes** for which it was collected - and **may not retain** such data for any longer then the period reasonably necessary to achieve those purposes.

Core Principles for Data Processing (cont'd)

- Ongoing obligations to ensure that the personal data being held is:
  - accurate;
  - complete; and
  - current.
- Security safeguards must be implemented –
  - as appropriate taking into account the nature and importance of the data at issue
  - more prescriptive standards may be issued by way of Ministerial resolution
- Rights of Data subjects - they may:
  - withdraw consent to the processing of their personal data;
  - object to certain processing activities;
  - issue requests for the deletion or correction of their personal data; and
  - request access to their personal data and related info about how / why it is being processed.
- Security breach notification requirements
  - apply to both processors and controllers
  - controllers to notify data subject **and** Ministry if breach is "*likely to cause serious damages*" to data or privacy of individual

Consent Requirements

- As a general rule – **consent** must be obtained from data subjects prior to processing
- No specifications as to particular form that consent must take
- For "***sensitive personal data***", however:
  - processing is prohibited unless advance approval is obtained from the Ministry
  - currently unclear what form this approval process will take
  - Ministry expressly reserves right to set additional precautions to protect sensitive personal data

Exemptions from the Law

- Generally - the Law **does not** apply to the processing of personal data:
  - by individuals in connection with personal or family matters; or
  - for official statistical purposes.
- **Controllers** are exempted from complying with certain aspects of the Law (including consent requirements) where the processing is occurring for:
  - carrying out a task related to public welfare.
  - implementing any legal obligation or order from a competent court.
  - protecting the vital interests of an individual.
  - ***achieving purposes of scientific research for public welfare.***
  - collecting information needed for investigating any crimes, upon an official request from the investigation bodies.

Exemptions from the Law (cont'd)

- The relevant public authorities may also decide to exempt processing activities from complying with certain aspects of the Law (including data subject consent) where the processing is for the purpose of:
  - protecting national and general security
  - protecting international relations of the State
  - protecting the economic or financial interests of the State
  - preventing any crime or collecting information about the same or investigating it

- Further details of the above arriving via pending Ministerial resolutions.

Cross Border Data Transfers

Article (15)

Subject to the obligations stipulated in this Law, the controller may not take any decision or procedure that may block the flow of personal data cross borders unless the processing of such data contradicts the provisions of this Law or may cause serious damages to the personal data or privacy of the individual.

Electronic Marketing Restrictions

Article (22)

*It is **prohibited** to make any **direct electronic communication with the individual for the purpose of marketing** without securing a **prior consent** from him.*

The electronic communication should demonstrate the identity of the initiator and proof for direct marketing purposes. The communication should include also a correct address that can be easily accessed and through which the individual can send a request to the initiator for the purpose of stopping such communications or withdraw his previous consent regarding the same.

Enforcement & Penalties

- Fines of up to QAR 5,000,000 (Five Million Riyals)
- Corporate entities may also be subject to fines where violations of the Law are committed by their agents or representatives "*in its name or for its account*"
- Individuals may file a complaint with the Ministry if rights under the Law are violated -
  - Ministry investigates
  - May issue a binding order to controller/processor to rectify situation
  - Controller/processor may file grievance to the Minister (within 60 days of order)
  - Minister will decide on grievance (within 60 days of it being submitted)
  - No response from Minister = deemed rejection of grievance
  - Minister's decision is final
- Ministry employees tasked with enforcing the Law will have the power of judicial/law enforcement officers and will have the power to seize and document any crimes related to violating the provisions of this Law.

Enforcement & Penalties (cont'd)

Article (28)

Any contract or agreement entered in violation to the provisions of this Law shall be deemed null and void.

But - how will this clause be interpreted?

- Void in whole or in part?
- Will this apply retroactively?
- Is there a threshold as to severity of the violation?
- What about situations where voiding the agreement further disadvantages the data subject?

Compliance - What to Do Next?

Compliance - Coming into Force & Grace Period

- The Law was published in the Gazette on 29 December 2016 and comes into force 30 days following the date of publication
- There is, however, a **6 month 'grace period'** for compliance
- So - what should you be focusing on during this time?

Your Compliance "To-Do List" - Start Thinking Best Practice!

The Law itself provides some guidance:

1. Review privacy policies and procedures before adopting any new processing operations.
2. Determine which processors will be in-charge of protecting personal data.
3. Train and familiarize your processors about best practice methods for personal data protection and compliance obligations under the Law.
4. Develop internal policies and rules for receiving and addressing complaints, data access requests, data correction or deletion requests, and make these available to individuals.
5. Develop internal policies and rules for effective management of personal data and for reporting any data security breaches.
6. Implement technologies to enable individuals to access their personal data, review and correct the same directly.
7. Conduct a comprehensive audit and review exercise to report on the extent of compliance with personal data protection obligations under the Law.
8. Ensure that processors consistently comply with instructions and take the required precautions for protecting personal data.

Thank you

Dentons & Co.
Level 18, Boulevard Plaa 2
Burj Khalifa District
PO Box 1756, Dubai
United Arab Emirates

Dentons & Co
Floor 15 Al Fardan Office Tower
61 Al Funduq Street
West Bay
PO Box 64057
Doha, State of Qatar

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Labs and the Nextlaw Global Referral Network. Dentons' polycentric approach and world-class talent challenge the status quo to advance client interests in the communities in which we live and work.
www.dentons.com