

# EU GDPR and Qatar Personal Data Privacy Law

Data Protection Officers' Network  
LexisNexis  
Al Sulaiti Law firm

# Disclaimer

- This presentation is intended for informational purposes only and does not constitute nor replace independent professional advice.
- Statements of fact and opinions expressed herein are those of the speakers individually and, unless expressly stated to the contrary, are not the opinion or position of the respective employers which do not endorse, approve or assume responsibility for the content, accuracy or completeness of the information presented.
- Attendees are not allowed to record this presentation.

What do you need to know about the EU  
GDPR?

# **GDPR - OBJECTIVES**

The objectives of the EU General Data Protection Regulation 2016/679, which replaces the EU Directive 95/46, are to protect personal data of natural persons in the EU and ensure that personal data are processed and transferred in accordance with the principles stated therein.

# CONTROLLER AND PROCESSOR

CONTROLLER	JOINT CONTROLLER	PROCESSOR
<p>The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines purposes (“why”) and means (“how”) of data processing</p>	<p>Entity that determines the purposes and means of data processing jointly with other Controllers</p>	<p>The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller</p>

# Principles relating to processing of personal data (Article 5 GDPR)

- Lawfulness, fairness and transparency
- Purpose limitation
- Data Minimization
- Accuracy
- Storage limitation
- Integrity, confidentiality
- Accountability

# Lawfulness of processing – Article 6 GDPR

Processing is lawful only if it is necessary:

- to **perform a contract** to which the data subject is a party
- to comply with **legal obligations** the controller is subject
- to protect **the vital interest** of the data subject or another natural person
- for the performance of a task carried out in **public interest**
- for the purpose of a **legitimate interest** of the controller (with restrictions in case the data subject is a child)
- The data subject has given his/her **consent**

# CONSENT OF THE DATA SUBJECT

- Freely Given
  - Specific
  - Unambiguous
  - Informed
- 
- **Clearly distinguishable** from the other matters
  - In an intelligible and easily accessible form, using clear and **plain language**
  - The data subject shall have the right to **withdraw** his or her consent at any time.



# GDPR – KEY CHANGES

- Privacy by design and by default
- Increased territorial scope (extra-territorial applicability)
- Consent
- New rights of data subject: data portability / profiling / right to be notified a breach
- New obligations of controller: accountability/implementation of security
- DPIA - data protection impact assessment
- DPO - data protection officer
- Transfer of data: adequacy/consent/derogation
- Penalties

# **DATA PROTECTION BY DESIGN AND BY DEFAULT**

- **PRIVACY BY DESIGN**

Controller must implement technical and organizational measures which are designed to implement data protection principles

- **PRIVACY BY DEFAULT**

Only personal data which are necessary for each purpose must be processed on a need-to-know basis

# TERRITORIAL SCOPE

## EXTRA-TERRITORIAL APPLICABILITY

GDPR applies to processing of personal data of data subjects done by:

- **Companies established in the EU**
- Companies not established in the EU **offering goods or services** within the EU or to individuals who are in the EU
- Entities **monitoring behaviour of individuals** who are in the EU as far as their behaviour takes place within the EU

# OBLIGATIONS OF THE CONTROLLER

- Demonstrate **compliance** with GDPR (Accountability)
- Provide **information** to Data Subject
- Carry out a Data Protection Impact Assessment (**DPIA**)
- Keep a **record** of processing activities
- Cooperate with the supervisory authority
- Implement measures to ensure an appropriate level of **security**
- Notify **data breach** to the supervisory authority
- Communicate data breach to the data subject
- Designate a **Data Protection Officer** (DPO)

# DATA PROTECTION IMPACT ASSESSMENT

## – DPIA (Art. 35 GDPR)

To be done prior to the processing, when there is a **high risk** to the rights and freedoms of natural persons

DPIA contains:

- a description of the **processing operations** and **purposes**
- an **assessment of the risks** to the rights and freedoms of data subjects
- the **measures** to address the risks

# DESIGNATION AND TASK OF THE DPO

DPO must be appointed:

- by a public authority
- when the controller's core activity entails a systematic monitoring of data subjects on a large scale
- When the controller processes special categories of data on a large scale

The DPO's functions include:

- a. to **inform** and advise the controller or the processor of their obligations pursuant to GDPR
- b. to **monitor** compliance with GDPR
- c. to **provide** advice where requested as regards the data protection impact assessment
- d. to **cooperate** with the supervisory authority

# RIGHTS OF THE DATA SUBJECT

- Right to **rectification** of inaccurate personal data
- Right to **erasure** (right to be forgotten) data that are no longer necessary in relation to the purpose for which they were collected and processed
- Right to **restriction of processing** (e.g. if accuracy is contested, the processing is lawful and the data subject opposed the erasure of personal data)
- Right to **data portability**: personal data given in a structured, commonly used and machine-readable format
- Right to **object** at any time to the processing
- Right to object to an **automated decision-making** including profiling

# Transfer of data to third countries or international organizations

A transfer of data to a different jurisdiction can be done only on the following basis:

Art. 45 GDPR - **Adequacy decisions**: the European Commission has decided that the third country ensures an adequate level of protection of personal data (a list of such countries is published on the Official Journal of the European Union)

Art. 46 GDPR - **Appropriate safeguards** (standard contractual clauses or binding corporate rules)

Art. 49 GDPR – **Derogations** for specific situations



# Fines up to 4% of the controller's worldwide turnover

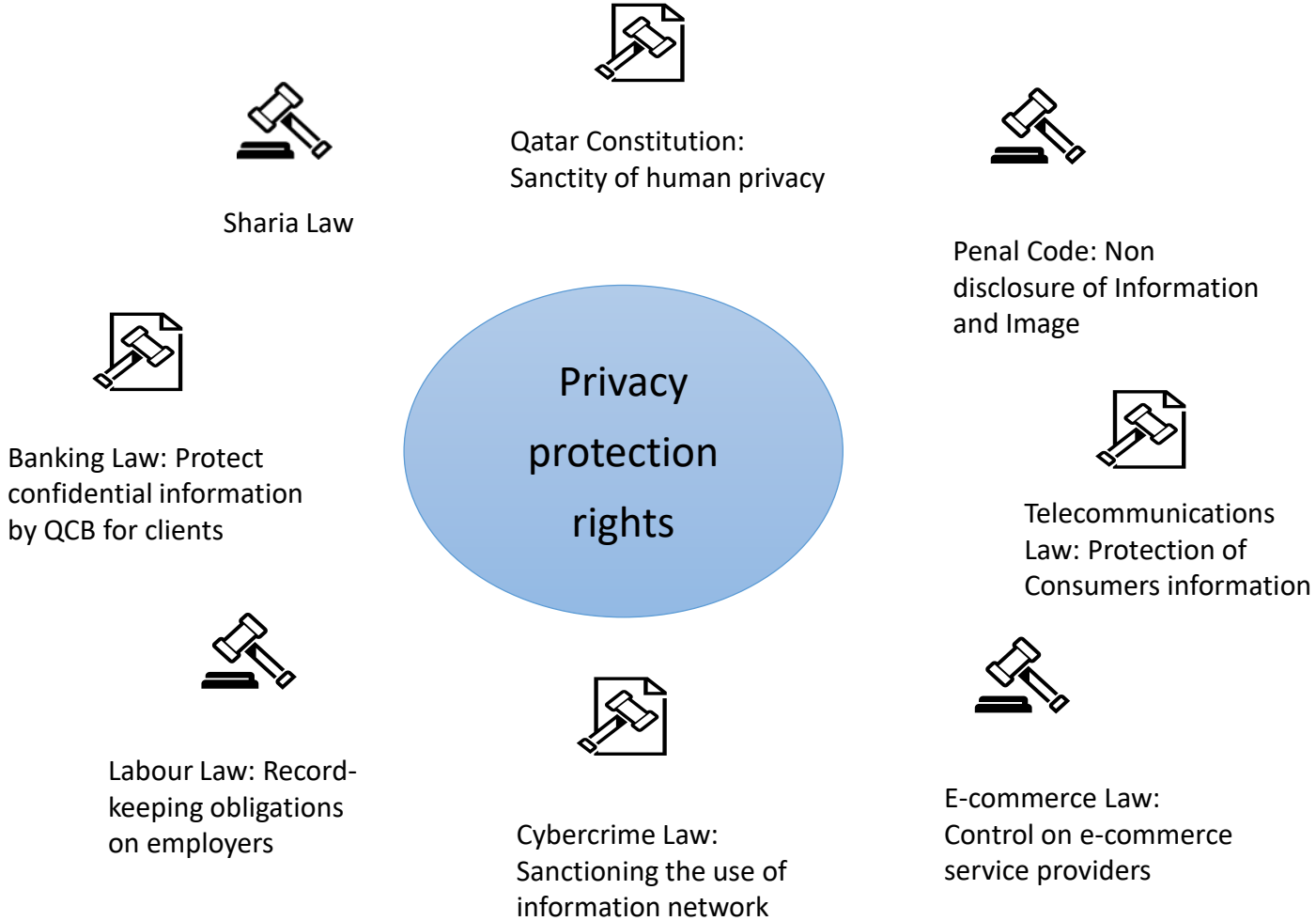
- From 10 Million to 20 Million

What do you need to know about the  
Qatar Personal Data Privacy Law?

# The New Personal Data Privacy Law

- First country in GCC
- Law n. 13/2016 concerning *privacy & protection of Personal Data*
- Grace period of 6 months
- DPA = Competent department of MoTC
  
- New safeguards that define Data processing similar to GDPR :
  - The right of individuals;
  - The responsibility of the Controller ;
  - Prohibition to process Sensitive Data;
  - Cross boarder transfers
  - Penalties up to 5 Million QAR

# Qatar current legal framework




Free Zone in QFC applying EU Data protection Directives 95/46 and EU GDPR

CONTROLLER	PROCESSOR	PROCESSING DATA	PERSONAL DATA
<p data-bbox="45 205 496 1025">“A controller is a natural or corporate person who individually or jointly with others, determines the method and purpose of processing personal data”.</p> <p data-bbox="45 1116 435 1248">The “why” and “How”</p>	<p data-bbox="529 205 919 716">“is a natural or corporate person who processes personal data for the controller”.</p> <p data-bbox="529 1102 945 1305">Public authority and Agency in GDPR</p>	<p data-bbox="998 205 1735 873">“is defined as one or several processes for personal data such as collecting, receiving, registering arranging saving preparing amending recovering using disclosing publishing transferring blocking deleting or cancelling personal data”.</p> <p data-bbox="998 1045 1717 1248">Whether or not by automated means (art. 2 of QDPL)</p>	<p data-bbox="1803 205 2430 716">“data of an individual whose identity is specific, or reasonably identifiable, either through such data or by combining it with any other data”.</p> <p data-bbox="1803 891 2456 1330">More factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person</p>

# Rights of Data Subjects

- Right to:
  - **Withdraw previous consent;**
  - **Object** to the processing on the grounds it is unnecessary, excessive, discriminatory, unfair or unlawful; or
  - Request for correction and /or **deletion** (ex when there is no justification for keeping such Data).
  - **Access and review** and being informed about the processing and/or any disclosures of their data.
- Right to be advised :
  - About **purpose** of the process
  - **Data breaches**
- Right to obtain **copy**



Right to be forgotten not explicit!

No right of Data Portability and Profiling!

# Data controllers' obligations

- Processing Data lawfully, transparently and fairly: (art. 8, 9, 10)
- Purpose limitation (art 9.2)
- Data minimisation (art. 9.3)
- Accuracy (art. 9.4)
- Storage limitation (art. 10)
- Integrity and Confidentiality (art. 8.2, 8.4, 11, 13, 14)
- Record only for the competent authority (art. 18)



# Special personal Data – Sensitive Data

- A **permit from Competent Authority** is required before processing personal data of a “special nature” such as:
  - racial or ethnic origin and religious affiliation
  - children
  - physical or mental health
  - criminal offences

No mention  
about  
Genetic and  
Biometric

- **Websites targeting children** must:
  - Post notices advising what data is being collected and how it will be processed and used
  - **obtain parent/guardian consent** to processing child data
  - comply with parent/guardian requests for information or to remove, erase or cease processing if requested by parent/guardian
  - participation in games, prizes, or other activities cannot be conditioned upon providing personal data

No age  
limit  
13-16  
years old



# GDPR vs Qatar Privacy Law

Principles	QPDPL	GDPR
The degree of implementation and details	Low (can be completed in Min. decision)	High
Biometric and genetic sensitive Data	NO	YES
Data portability and profiling	NO	YES
Threshold for children parental consent (13-16 years old)	NO	YES
DPO for companies	NO	YES
Record keeping	Only for MoTC	Both for DPA & companies
DPIA request and privacy by design & default	YES but Not explicitly	YES clearly defined
Electronic communications for direct marketing: prohibited unless prior consent obtained	YES	NO
Cross-border transfers authorized	YES (unless against the Law & cause harm to Data S.)	YES (more detailed)
Fines for Non Compliance	1 to 5 Million QAR	4% of worldwide annual Turnover or 20 Million Euros

# Future challenges – the implementation process

## **For the Ministry:**

- Create an effective DPA
- Establish processes and procedures to implement and enforce the Law
- Create awareness for Data Subject and companies

## **For the companies and other institutional bodies in Qatar:**

- Comply with the general principles of the Law
- Evaluate the impact of the GDPR & QPDPL on the processing activities
- Collect consent when it is appropriate
- Segregate types of Data
- Record the process
- Implement security safeguards

How to comply?

# Preliminary steps

1. Assess the current situation – Where we are NOW? Why do we process personal data (purpose)? How do we process data?
2. Identify areas for improvement
3. Decide what do you need to comply and define steps – Where do we want to be?
4. Analyze how your company moves from 1 to 3 – How to get there?
5. Do it! (audit, assess, coordinate, implement)

# Example:

Activity of the Company PRODUCT	Data TYPE Personal Data Sensitive Data	SHARED Processors, 3 <sup>rd</sup> parties	PURPOSE	LOCATION
Online Magazine	IP Address	Yes	To deliver the magazine	EU – Shared parties outside EU
Oil and Gas	Employee's personal Data (including finger prints)	Yes	Monitor their activities (check in and out)	Qatar
Airplane company	Passengers Data	YES	travel	Qatar, EU, US... wordwild

# Practical compliance tools

1. Assess your processing and identify the required safety measures to protect data
2. Implement a DP system ensuring adequate protection of personal data
3. Identify a lawful purpose to process personal data
4. Inform data subjects about the purpose of processing and their rights
5. Request consent if needed
6. Provide data subjects with privacy notice (information on purpose of processing, data controller and processor and others (articles 13 and 14))
7. Sign a processing agreement with your processor
8. Include a binding and enforceable dp clause in all contracts
9. Transfer data only in accordance with GDPR (standard data protection clauses/binding corporate rules/codes of conduct)

# GO FURTHER!

- Designate a qualified DPO or a compliance manager
- Keep record of your processing activities
- Prioritize your actions
- Organize your internal auditing process
- Be accountable: make sure to comply and to be able to demonstrate compliance
- Report processing of sensitive data to MoTC

# Thank you!

Luigia Ingianni : [l.ingianni@qfc.qa](mailto:l.ingianni@qfc.qa)

Oriane Barat: [obarat@motc.gov.qa](mailto:obarat@motc.gov.qa)