Webcast

Data privacy in Qatar: What you need to know

pwc

With you today

Issa Habash
Partner, Qatar Other Assurance Services Leader
PwC Middle East

Phil Mennie
Partner, Middle East Data Privacy Leader
PwC Middle East

Nakul Srivastava
Director, Qatar Digital Trust Services Leader
PwC Middle East

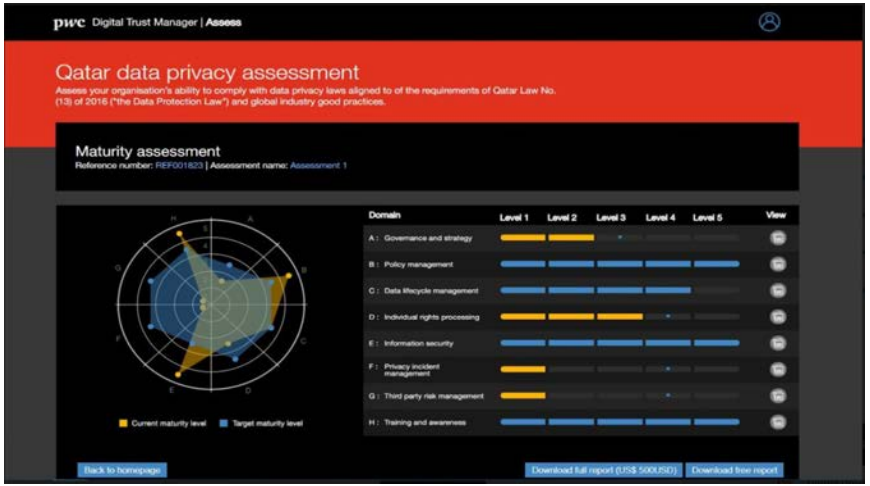
Richard Chudzynski
Senior Manager, Data Protection and Privacy Leader
PwC Legal Middle East

Our focus for today

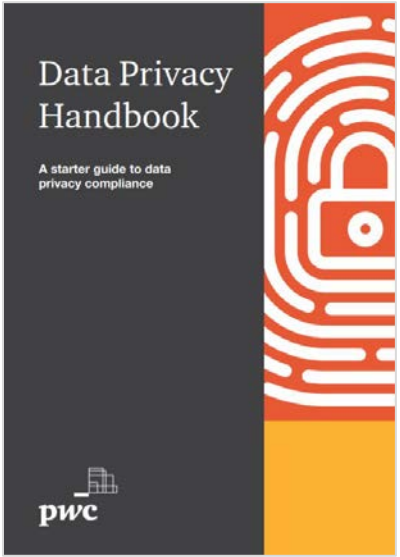
Welcome	**Data privacy 101**	**Understanding the new data privacy law**
10 steps to an effective data privacy programme	**Q&A**	

Resources

Qatar data privacy law online self assessment



Data Privacy Handbook



Quick poll

- Are you aware about the recent data protection guidelines issued by the MoTC?
- Do you have an existing data privacy programme?

1

Data privacy 101

Why is data privacy important?

Competitive advantage

Organisations are finding efficient and economical ways to run their businesses which involve transferring data outside of their jurisdictions and are using data analytics to create new revenue streams.

Consumer Trust

Organisations need new mechanisms to build consumer trust and confidence as they address emerging challenges in business, risk management, and compliance.

Interconnected world

Traditional ways of doing business are no longer valid in an increasingly interconnected world, with people and information being spread across multiple countries.

Privacy regulation

Regulatory bodies are taking an increasingly tough stance on privacy, imposing heavy fines on breaches for violations of individuals right to privacy.

Data privacy laws in the Middle East

Constitutional codes
The constitutions of some Middle East countries recognise the individual's right to privacy under certain conditions.

Sectoral laws
Elements of privacy are embedded within several laws pertaining to specific industry sectors.

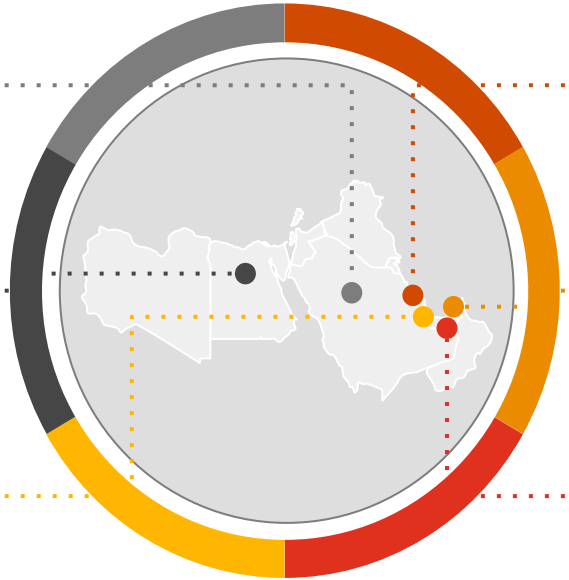
Imminent laws
Some countries in the region have drafted privacy laws for a few years which might come into effect in the near future.

Regulations in the Middle East

In draft
KSA
Data protection and freedom of information law

Enacted
Egypt
2020 data protection law

Enacted
Bahrain
Personal data protection law No. 30 of 2018



Enacted
Qatar
Data protection law No. (13) of 2016 - Personal Data Privacy Protection Law (PDPPL)

Enacted
UAE
DHCC Health Data Protection Regulation No 7 2019

In draft
UAE
UAE federal draft data protection law

With the exception of two GCC countries which have recently enacted data protection laws, overarching privacy laws common in some parts of the world do not exist in the Middle East. However the right to privacy is recognised and afforded to individuals through several means:

Risks to the organisation

What risks can the organisation face?

Organisations that fail to protect personal data and comply with data privacy regulations aren't just risking financial penalties. They also risk operational inefficiencies, intervention by regulators and most importantly permanent loss of consumer trust.

Regulatory

Regulators may require the provision of information, conduct audits, and obtain access to premises if they determine it is necessary.

Reputational

Non-compliance with the the law could result in brand damage, loss of consumer trust, loss of employee trust and customer attrition.

Financial & Criminal

Fines and, in some countries potential prison sentences, could be enforced depending on the violation. You may also experience loss of revenue and high litigation and remediation costs.

Operational

Data subjects can impose data processing bans and order the correction of an infringement. This could result in restricted operations and invalidated data transfers.

What is personal data?

Personal data

Personal data is any **information that can identify a living person**.

Personal data	Non-personal data
Name and surname	An organisation's corporate registration number
ID card number	Mailboxes such as info@pwc.com
Online identifiers (e.g. IP addresses)	
CCTV footage	

Sensitive personal data

Some personal data is considered **sensitive**, as it **could cause serious harm to the individual if leaked or misused**.

Sensitive personal data as per PDPPL

- Racial or ethnic origin
- Physical or mental health
- Political or religious beliefs
- Children and family members
- Trade union membership
- Criminal offences & court proceedings

It's important to differentiate between personal data and sensitive personal data because the processing of sensitive personal data usually requires additional safeguards to be in place.

How is data privacy affecting organisations?

Data inventory

Mandatory data inventorying and record keeping of all internal and third-party processing of European personal data.

Breach notification

Mandatory data-breach notification to regulators and individuals whose information is compromised.

Right to access

Comprehensive individual rights to access, correct, port, erase, and object to the processing of their data.

Impact assessment

Routine data-protection impact assessments for technology and business change.

Governance

Mandatory data protection officers and an overall rethinking of privacy strategy, governance, and risk management.

Third parties

How third parties handle personal data represents a risk and administrative burden to update and negotiate contracts.

Seven key data privacy principles

Transparency, honesty and respect for human dignity

You should always process personal data in a fair, lawful and transparent manner, in line with the requirements of the applicable data privacy laws.

Purpose Limitation

You should only process personal data for a specified and lawful purpose. You cannot use the data for another purpose unless conditions are met.

Data Minimisation

You must ensure you are only processing the personal data which you truly need to conduct your business and nothing more.

Accuracy

You should ensure personal data is kept up to date, and that necessary measures are in place for correcting and updating inaccurate data.

Storage Limitation

You must not keep personal data for longer than you need it. It should be securely destroyed after the defined retention period.

Integrity & Confidentiality

You must implement adequate security controls to ensure that personal data is protected against loss, destruction or damage.

Accountability

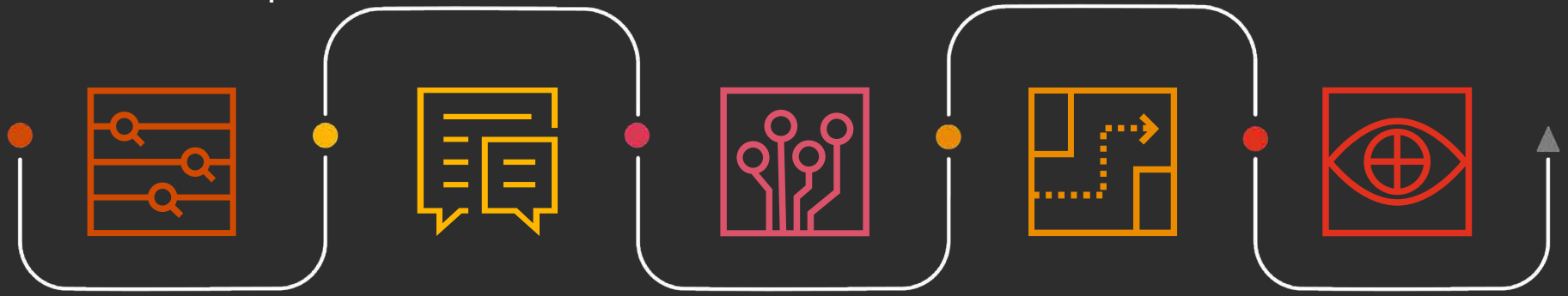
You must have appropriate measures and records in place to be able to demonstrate your compliance.

Five step approach to compliance

Assess current capabilities

Design the future state

Operate and sustain



Risk analysis and data discovery

Establish your personal data footprint:

- types and scale of data held
- jurisdictions they fall within
- personal data risks you face

Gap assessment

Assesses your current capabilities against relevant legal requirements for your current and future uses of personal data. It will help identify the gaps, and where improvements can be made.

Target operating model and programme design

Define and establish the ongoing governance structure in order to coordinate, operate and implement the remediation activities.

Programme implementation

Implementation will be carried out according to the specific programme designed according to the your gaps and requirements.

Ongoing operations and monitoring

Establish the necessary ongoing compliance mechanisms to promote continued accountability.

PwC's data privacy programme

PwC's data privacy framework

Strategy, Governance & Accountability

- Data Protection Designation
- Governance Structure
- Training & Awareness

Data Subject Rights & Processing

- Data subject rights (e.g. Right to Rectification / Right to be Forgotten, Automated Decision - making)

Privacy Notice & Policy Management

- Policies, Standards & Guidelines.
- Transparent & Concise Communicatio n

Risk Management & Compliance

- Regulatory Compliance Monitoring
- Risk Identification, Mitigation & Reporting
- Privacy Impact Assessment

Data Lifecycle Management

- Data Classification, Inventory, Sources, Flow/Maps
- Data Quality
- Privacy by Design (PbD)

Incident Response & Breach Management

- Breach Identification
- Breach Notification
- Incident Response

Third Party Risk Management

- Cross-border Transfers & Safeguards
- Contracting
- Monitoring

Data Security

- Security
- Disaster Recovery, Business Continuity and Backup

2

Understanding the new data privacy law

GDPR versus Qatar Data Protection Law

Key:
- Similar
- Absent
- Broader
- Narrower

Below is a comparison of the PDPPL as against the European Union General Protection Law (GDPR).

	GDPR		PDPPL
Material and Territorial Scope	Personal data ***collected*** in the EU / EEA i.e."EU personal data"	><	Personal Data processed in Qatar
Data Subject Rights	Right to access all EU personal data processed	=	Comprehensive rights exist including the right to access, deletion and rectification.
Right to portability	Must provide useable copy of EU personal data to third party	=	Must rectify any inaccurate disclosure of personal data to a third party
Right to stop processing	Right to withdraw consent or otherwise stop processing of EU personal data	=	Right to withdraw consent or otherwise stop processing of personal data
Rights response	1 month with potential extension by 2 additional months	=	30 calendar days with potential extension by 2 additional months
Cross-border transfer	Permitted under specific conditions and if adequate levels of data protection are provided.	><	Controllers may not take measures to limit cross-border data transfers unless high risk to privacy or personal data. Controllers should document assessment of potential risk and send notification to regulatory authority.
Governance	Appoint a DPO and a lead supervisory authority under certain conditions. Roles & responsibilities defined by the regulation.	><	No registration requirements and no requirement to appoint DPO.
Incident and breach response	Disclosure of incidents and data breaches without undue delay and within 72 hours of the breach	><	Controller must report breaches to regulator, CDP of the MOTC, and data subject, where likely to cause damage to data subject.
Penalties	Up to **€20m** or **4% of global annual revenues**.	><	Fines of between **1 million - 5 million QAR.**

Quick poll

- Does your organisation have adequate technical information security controls to protect personal data?
- Do you plan on making any changes to the way your organisation handles personal data in the coming months?


3
Ten steps to an effective
data privacy programme

Ten steps to an effective data privacy programme

1. Appoint a Data Protection Officer

2. Maintain a personal data register

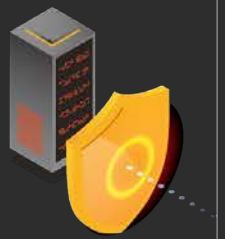
3. Notify purpose and seek consent

4. Respond when individuals ask about their personal data

5. Enforce security mechanisms

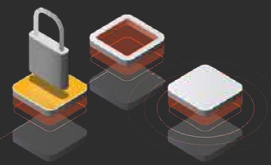
Ten steps to an effective data privacy programme

6 Embed data privacy into your systems, processes and services



7 Notify data breaches

8 Manage third parties



9 Protect personal data when transferring overseas

10 Communicate your data protection policies, practices and processes

4

Q&A

Contact us

Issa Habash
Partner, Qatar Other Assurance Services Leader

PwC Middle East
issa.habash@pwc.com

Phil Mennie
Partner, Middle East Data Privacy Leader

PwC Middle East
phil.mennie@pwc.com

Nakul Srivastava
Director, Qatar Digital Trust Services Leader

PwC Middle East
nakul.srivastava@pwc.com

Richard Chudzynski
Senior Manager, Data Protection and Privacy Leader

PwC Legal Middle East
richard.chudzynski@pwc.com

Thank you

pwc.com