

Webcast

Data privacy in Egypt: What you need to know



© 2020 PwC. All rights reserved

With you today



Nabil Diab
Partner, Egypt
PwC Middle East



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



Richard Chudzynski
Legal
PwC Middle East



Tamer Amin
Director, Egypt
PwC Middle East



Our focus for today

Welcome

**Data privacy
101**

**Understanding
the new data
privacy law**

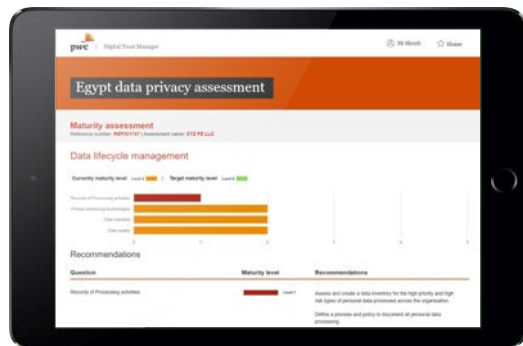
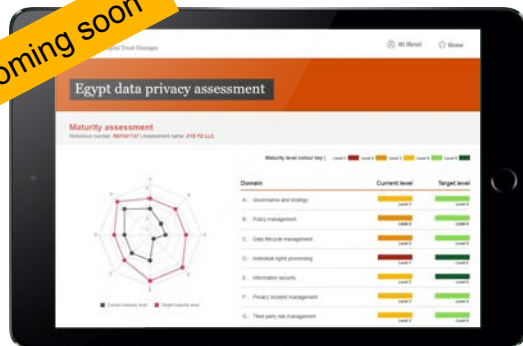
**10 steps to an
effective data
privacy
programme**

Q&A

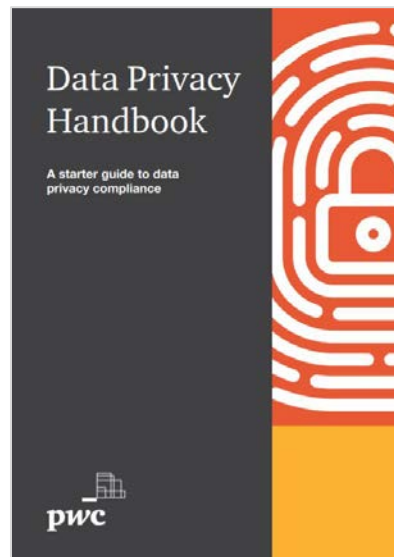
Resources

Egypt data privacy law online self assessment

Coming soon



Data privacy handbook





Quick poll

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Traditional ways of doing business are no longer valid in an increasingly interconnected world, with people and information being spread across multiple countries.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

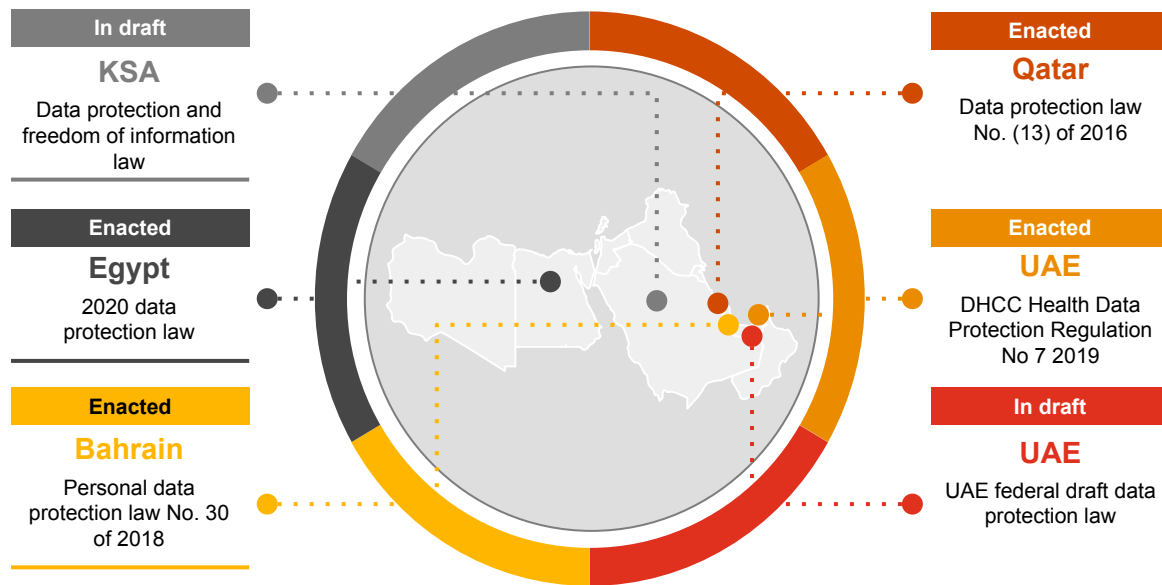
- Elements of privacy are embedded within several laws pertaining to specific industry sectors.



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



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



Name and surname



ID card number



Online identifiers (e.g. IP addresses)



CCTV footage

Non-personal data



An organisation's corporate registration number



Mailboxes such as info@pwc.com

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



Racial or ethnic origin



Physical or mental health



Political or religious beliefs



Sex life or sexual orientation



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



Lawfulness, Fairness & Transparency

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

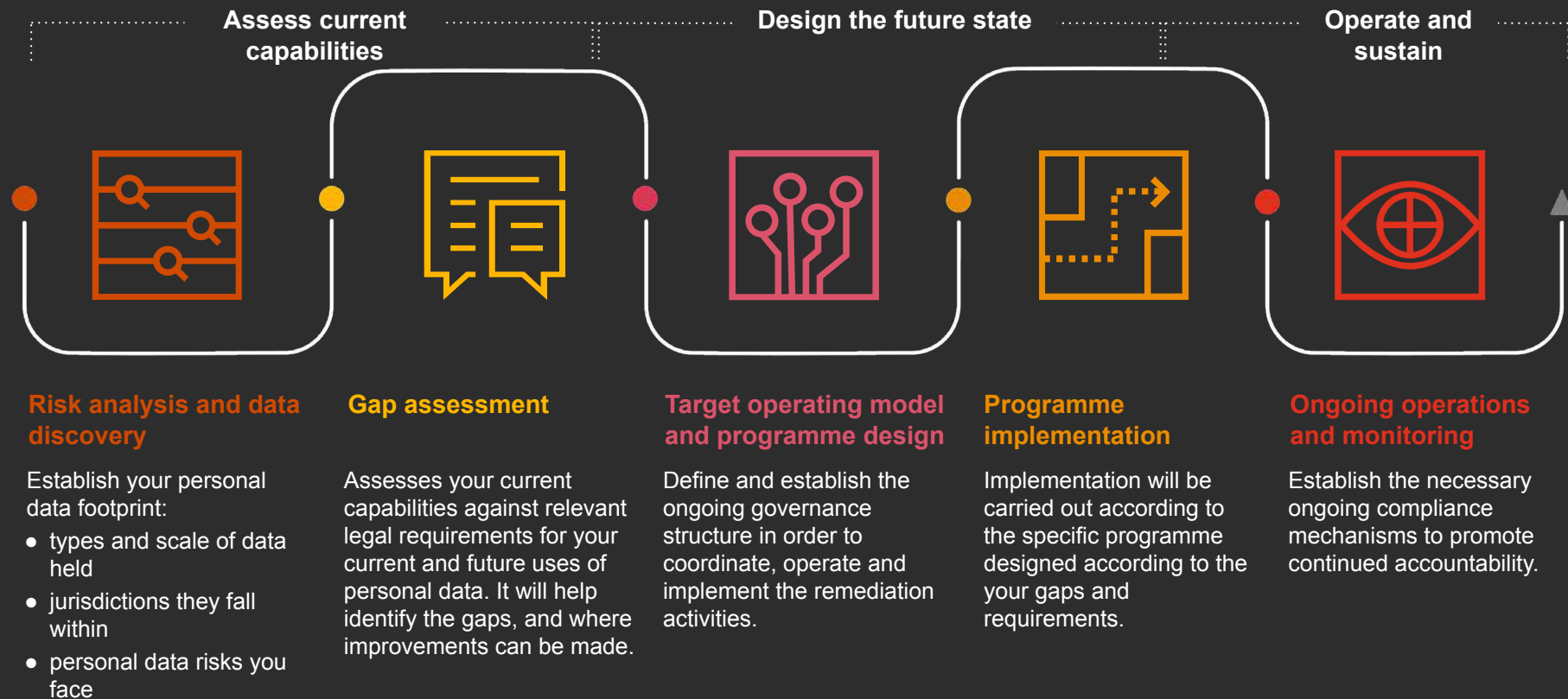
You must implement adequate security controls to ensure that personal data is protected against loss, destruction or damage.



Accountability

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

Five step approach to compliance



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 Communication



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* Egypt Data Protection Law

Key:

Similar	=
Absent	✗
Broader	()
Narrower	⌋ ⌈

Below is a comparison of the Egypt data protection law as against the European Union General Protection Law (GDPR).

	GDPR		Egypt Data Protection Law
Scope	Processed EU personal data	()	Personal data for Egypt residents processed through electronic means in part or full. The law excludes the Central Bank of Egypt (CBE) and most of the entities subject to the supervision of the CBE.
Right to access	Right to access all EU personal data processed	⌋ ⌈	Right to access personal data for a fee. Fee to be published by the Center (Authority) in due course.
Right to portability	Must export and import certain EU personal data in a user-friendly format	✗	Not included in Egypt Personal Data Protection Law.
Right to correction and erasure	Right to correct errors in EU personal data processed or erase EU personal data under certain conditions	=	Right to correct errors in personal data processed or erase personal data under certain conditions.
Right to stop processing	Right to withdraw consent or otherwise stop processing of EU personal data at any time	=	Right to withdraw consent, opt-out of direct marketing and object to processing that contradicts the fundamental rights and freedoms of the Data Subject.
Right to stop automated decision-making	Right to require a human to make decisions that have a legal implications	✗	Not included in Egypt Personal Data Protection Law.
Response time for data subject requests	1 month with potential extension by 2 additional months	()	Decision on a request to be made within 6 working days. No time limit to respond.
Cross-border transfers	Permitted under specific conditions and if adequate levels of data protection are provided	()	Subject to obtaining a relevant license or permit from the Center.
Governance	Appoint a DPO and a lead supervisory authority under certain conditions. Roles & responsibilities clearly defined	⌋ ⌈	Appoint a Data Protection Supervisor. Obligations clearly defined in the law.
Incident and breach response	Where required, disclosure of incidents and data breaches without undue delay and within 72 hours of the breach	⌋ ⌈	Disclosure of data breaches within seventy-two hours. If the breach relates to national security protection considerations, the notification shall be immediate. [Notify the Data Subject about the breach within three days.
Regulator enforcement penalties	Fines up to the greater of EUR20m or 4% of global annual revenues	()	Ceiling of Five million Egyptian Pounds fine with potential sentence of imprisonment for more than 6 months.

3

Ten steps to an effective
data privacy programme

Ten steps to an effective data privacy programme

Appoint a Data Protection Officer

1



Maintain a personal data register

2



Notify purpose and seek consent

3



Respond when individuals ask about their personal data

4



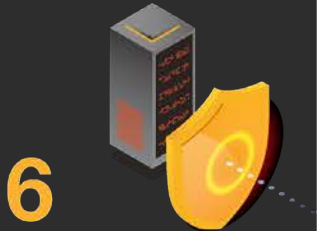
Enforce security mechanisms

5



Ten steps to an effective data privacy programme

Embed data privacy into your systems, processes and services



Notify data breaches



Manage third parties



Protect personal data when transferring overseas



Communicate your data protection policies, practices and processes





4

Q&A



Quick poll

Contact us



Nabil Diab
Partner, Egypt
PwC Middle East

PwC Middle East
nabil.diab@pwc.com



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

PwC Middle East
phil.mennie@pwc.com



Richard Chudzynski
Legal
PwC Middle East

PwC Middle East
richard.chudzynski@pwc.com



Tamer Amin
Director, Egypt
PwC Middle East

PwC Middle East
tamer.amin@pwc.com



Thank you

[pwc.com](https://www.pwc.com)

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with over 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com. Established in the Middle East for 40 years, PwC has 22 offices across 12 countries in the region with around 5,200 people. (www.pwc.com/me).

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

© 2020 PwC. All rights reserved