

Navigating cross-border data transfers

Overview of key regulations in the Middle East

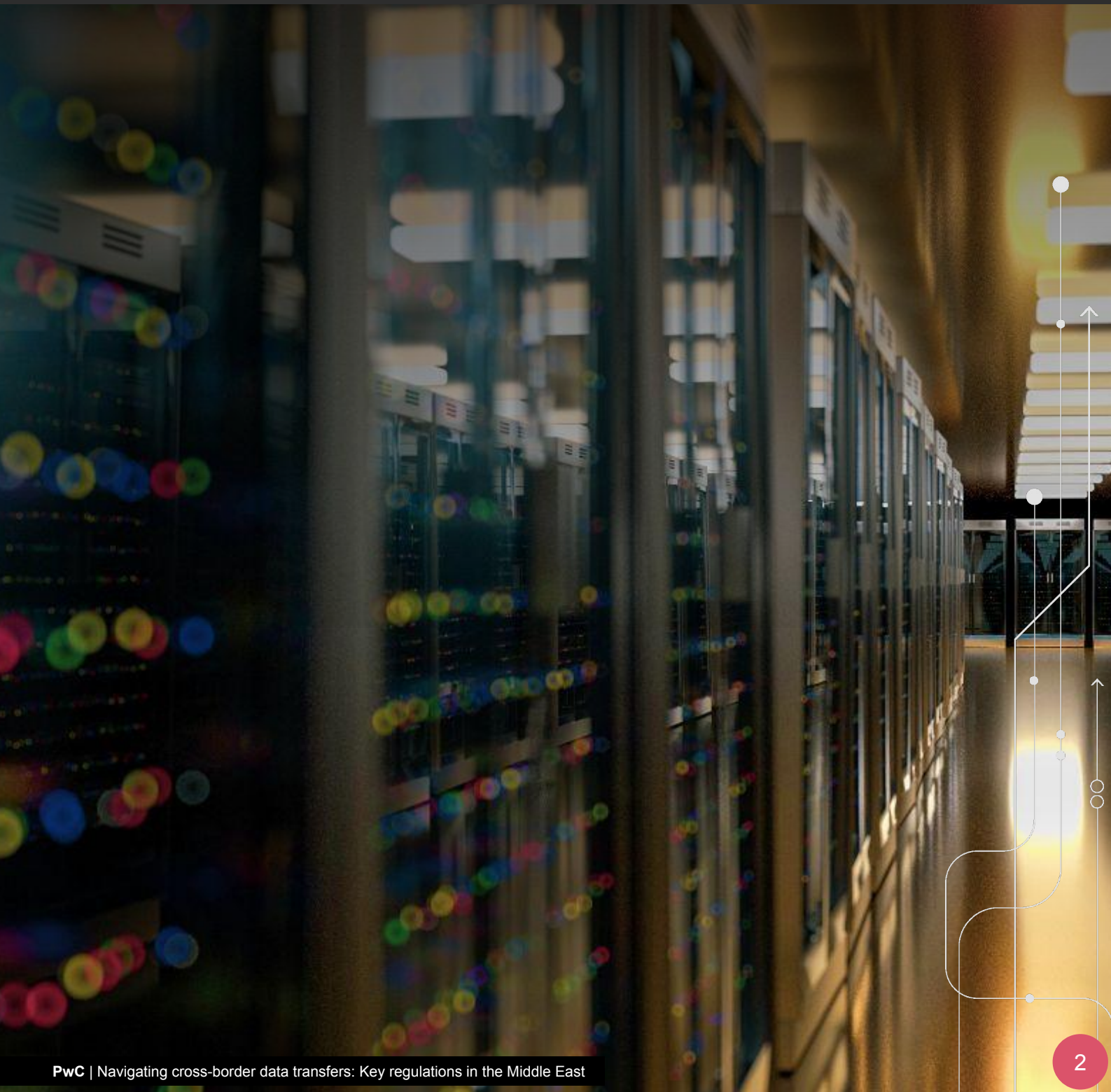
In an increasingly interconnected region, the movement of personal data across borders has become a crucial concern for individuals, governments, and organisations. As countries in the Middle East implement stringent data protection laws, businesses must adapt to ensure compliance and maintain trust.





Introduction:

Cross-border data transfer regulations are critical for maintaining the integrity and security of personal data as it is shared internationally. These regulations ensure that personal data is handled in a manner that respects the privacy rights of individuals and complies with local and international legal standards. Organisations must navigate these complex requirements to avoid legal repercussions, safeguarding their reputation as well as the privacy of the individuals. Following the recent enforcement of the Saudi Personal Data Protection Law (PDPL), this guide provides a comprehensive overview of key regulatory requirements for cross-border data transfers in selected Middle Eastern countries, focusing on personal data protection laws.



Saudi Arabia

Key laws and regulations in the personal data protection area

- Personal Data Protection Law (“**PDPL**”).
- Implementing Regulation of the PDPL.
- Regulation on Personal Data Transfer Outside the Kingdom.

Key rules on the cross-border data transfer

Key regulatory authority:

Saudi Data & Artificial Intelligence Authority (SDAIA).

Need for authorisation:

No authorisation of the regulatory authority is required for cross-border transfers.

Key Requirements:

- **Several lawful bases:** To transfer personal data it is necessary to establish the lawful basis for the processing of personal data (from the list specified in Article 5 and Article 6 of the PDPL) and for disclosure of personal data (from the list specified in Article 15 PDPL). Lawful bases include inter alia consent and legitimate interest.
- **Countries with adequate level of protection:** Unless the transfer is to a country on the SDAIA “white list”, the transfer will be permitted only subject to specific safeguards and exceptions.

Please see the detailed PwC Middle East guide on the cross-border data transfer requirements in Saudi Arabia ([Part 3 of the PDPL series](#)).

PwC Middle East key insights

Regulation on personal data transfer outside the Kingdom generally restricts such transfers. It is advisable to consider options for storing personal data within the territory of the Kingdom.

United Arab Emirates

Key laws and regulations in the personal data protection area

- Federal Decree by Law No. 45 of 2021 Concerning the Protection of Personal Data (“Law”).
- Legal instruments regulating personal data protection (including cross-border data transfers) in special zones, for instance:
 - DIFC Data Protection Law and data protection regulations.
 - ADGM Data Protection Regulations 2021.

These special zone legal instruments are not described in this guide.

Key rules on the cross-border data transfer

Regulatory authority:
UAE Data Office.

Need for authorisation:

No authorisation of the regulatory authority is required for cross-border transfers.

Key requirements:

- **Countries with adequate level of protection:** As a general rule, a transfer is allowed to countries providing adequate protection to the personal data (Article 22 of the Law). The list of countries with an adequate level of protection will be approved by the UAE Data Office. No such a “white list” currently exists.
- **Bilateral or multilateral agreement:** The importing country may be also considered as having an adequate level of protection, if it has signed with the UAE a bilateral or multilateral agreement on protection of personal data.
- **Transfers to non-adequate countries:** Transfers to non-adequate countries (those not on the white list) are allowed in specific cases (Article 23 of the Law):
 - In the absence of data protection laws in the importing country, the transfer to it will be allowed under an agreement with the data importing entity, whereby such an entity undertakes to implement the data protection rules of the UAE Law.

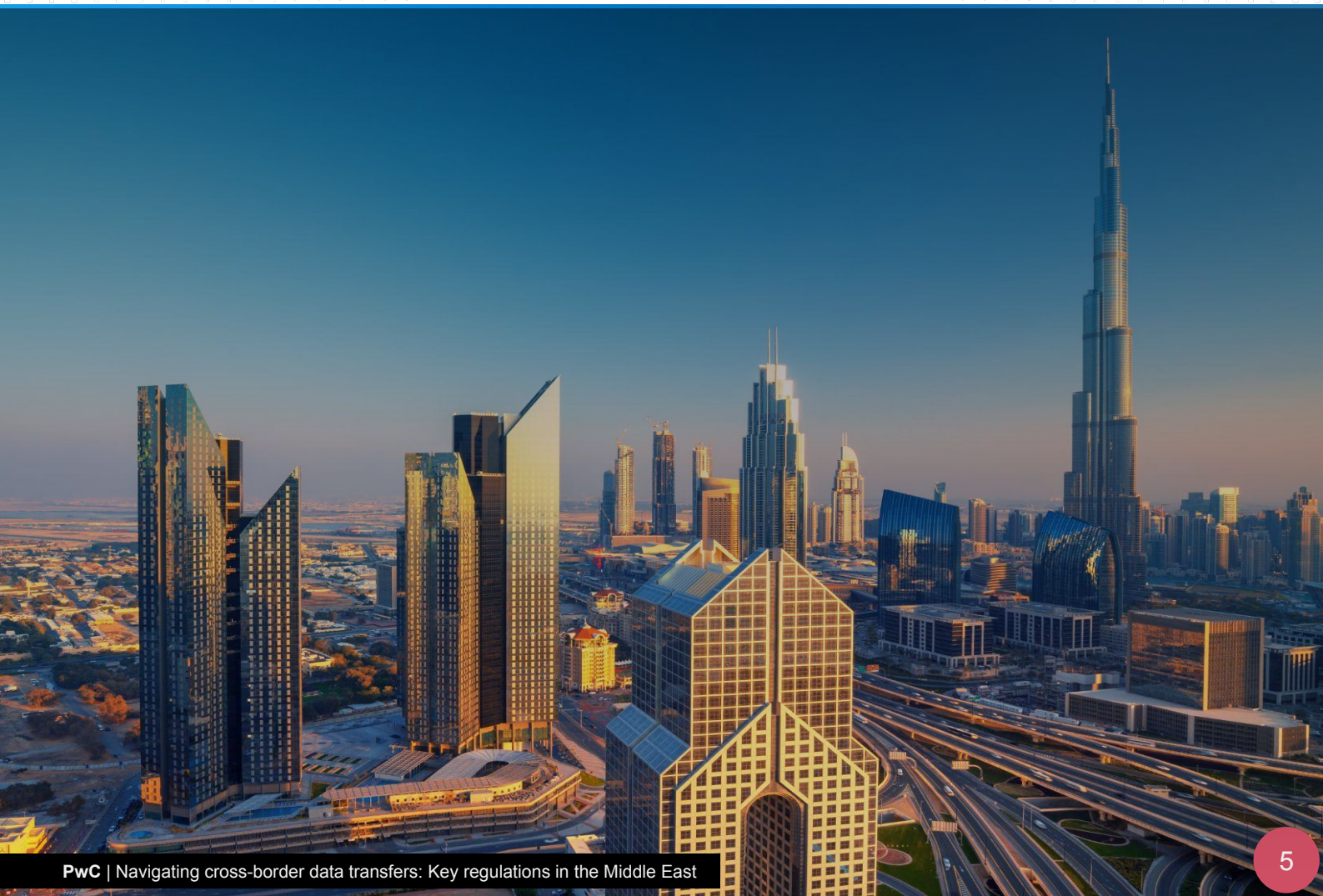
United Arab Emirates

Key rules on the cross-border data transfer *(continued)*

- The entity has express consent from the data subject to transfer their personal data outside of the UAE.
- The transfer is necessary for obligations, and ascertaining, exercising, or defending rights before judicial authorities.
- The transfer is necessary for the entry into or the performance of a contract between the controller and the data subject, or between the controller and a third party for the interests of the data subject.
- The transfer is necessary for the performance of an act relating to international judicial cooperation.
- The transfer is necessary for the protection of public interest.

PwC Middle East key insights

- It is expected that the executive regulations shall specify additional important provisions and controls relevant to cross-border data transfers.
- As of today the Law has not started to be enforced.



Qatar

Key laws and regulations in the personal data protection area

- Law No. 13 of 2016 concerning Personal Data Protection (“**Law**”).
- Additional guidelines on the Law are published by the Ministry of Transport and Communications.
- Qatar Financial Centre has its own rules and regulations on personal data protection (these rules and requirements are not addressed in this guide).

Key rules on the cross-border data transfer

Regulatory authorities:

Ministry of Transport and Communications; National Cyber Security Agency.

Need for authorisation:

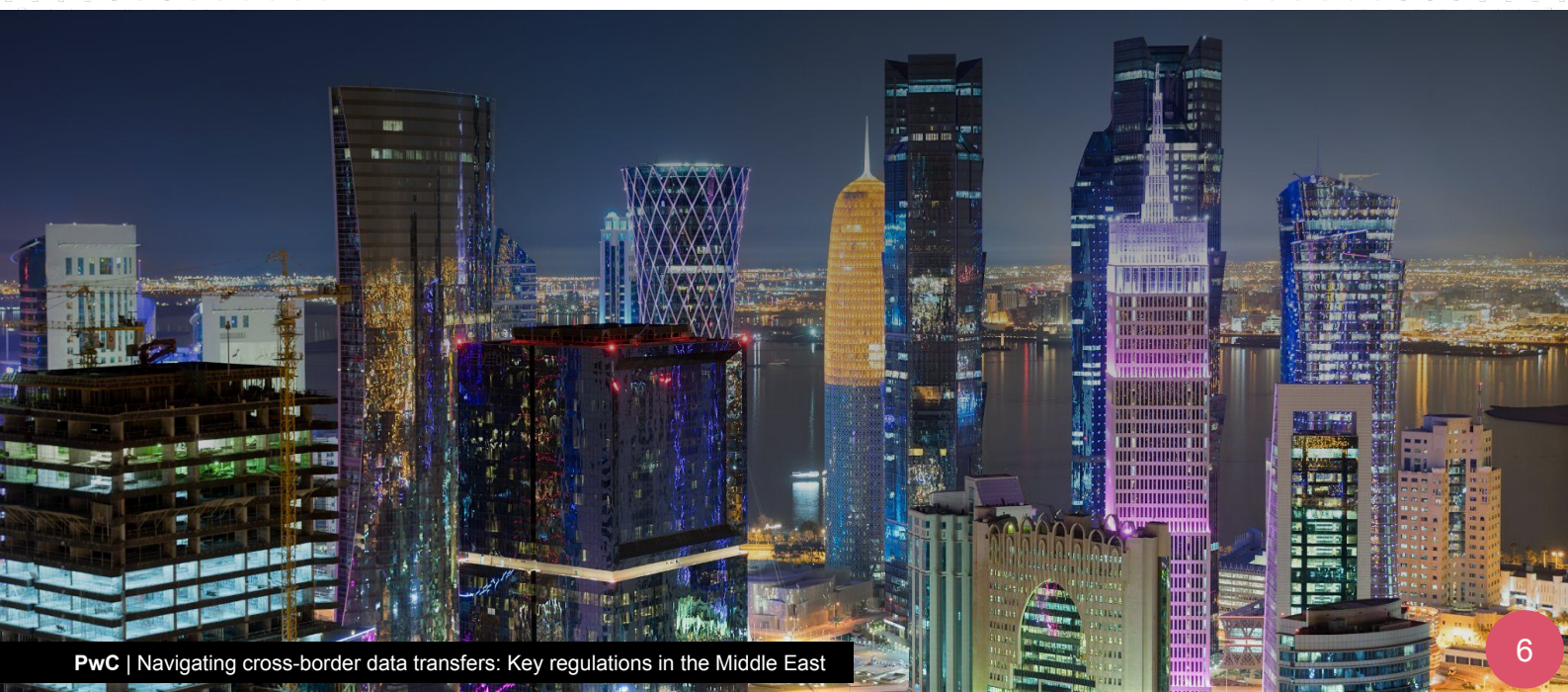
Required for transfer of data of special nature.

Key requirements:

- **Data of special nature:** Processing of data of special nature, such as health and children’s data, including its transfer, is allowed only after obtaining permission from the Ministry of Transport and Communications (Article 16 of the Law).
- **Data protection impact assessments:** Ministry of Transport and Communications guidelines recommend performing a data protection impact assessment before arranging any cross-border data transfer.

PwC Middle East key insights

- The Law does not substantially restrict cross-border transfers, unless the transfers relate to special categories of data.
- The Law does not describe in detail safeguards and requirements for cross-border data transfers. It is recommended that transfers are undertaken under the contract between data exporting and importing entities, outlining requirements to protection of personal data.



Bahrain

Key laws and regulations in the personal data protection area

- Law No. (30) of 2018 with respect to Personal Data Protection Law (“**Law**”).
- Executive Order No. (42) of 2022, regarding the transfer of personal data outside the Kingdom of Bahrain (“**Order**”).

Key rules on the cross-border data transfer

Regulatory authorities:

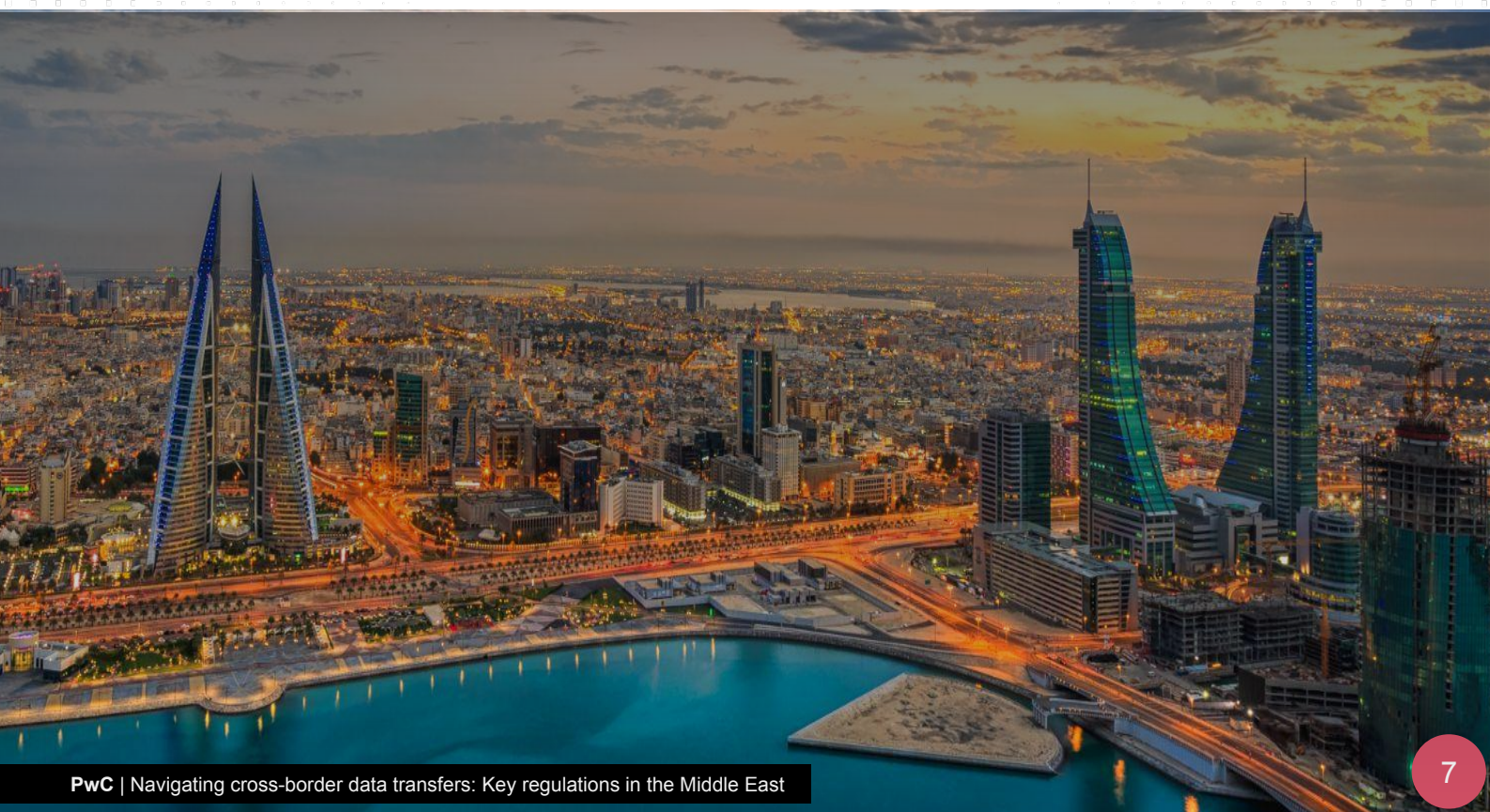
Ministry of Justice, Islamic Affairs and Waqf.

Need for authorisation:

Case-by-case authorisations are required for data transfers to the countries not specified on the “white list” – unless a specific lawful basis for the transfer is established.

Key requirements:

- **Countries with adequate level of protection:** The data transfer is generally only allowed to the countries providing adequate protection to the transferred data, according to Article 12 (1) of the Law. The list of countries (“white list”) is specified in the Order (83 countries as of now).
- **Transfers to non-adequate countries:** Transfers to non-adequate countries are allowed subject to obtaining authorisation from the authority for each case, as per Article 12 (2) of the Law and Article (3) of the Order. The authority will determine if there is a sufficient level of protection in respect of the personal data being transferred.



Bahrain

Key rules on the cross-border data transfer *(continued)*

- The transfers to countries without an adequate level of protection can be carried in the following cases (Article 13 of the Law):
 - If the data subject consents to the transfer.
 - If data is transferred from a public register, where such a register is required under the law.
 - Concluding or performing a contract between the data subject and data controller.
 - Concluding or performing a contract between the data controller and any third party in the interest of the data subject.
 - In the vital interest of the data subject.
 - Execution of an obligation under the law.
 - In preparation of a file or defence of a legal claim.

It is not completely clear whether in the above cases the authorisation of the regulatory authority is still required for the transfer.

PwC Middle East key insights

- Bahrain is currently the only country in the GCC region that has adopted a list of countries with adequate level of protection of personal data.



Oman

Key laws and regulations in the personal data protection area

- Personal Data Protection Law (“**Law**”).
- Executive Regulation of PDPL (“**Regulation**”) - fully enforceable from February 2025.

Key rules on the cross-border data transfer

Regulatory authority:

Ministry of Transport, Communications, and Information Technology.

Need for authorisation:

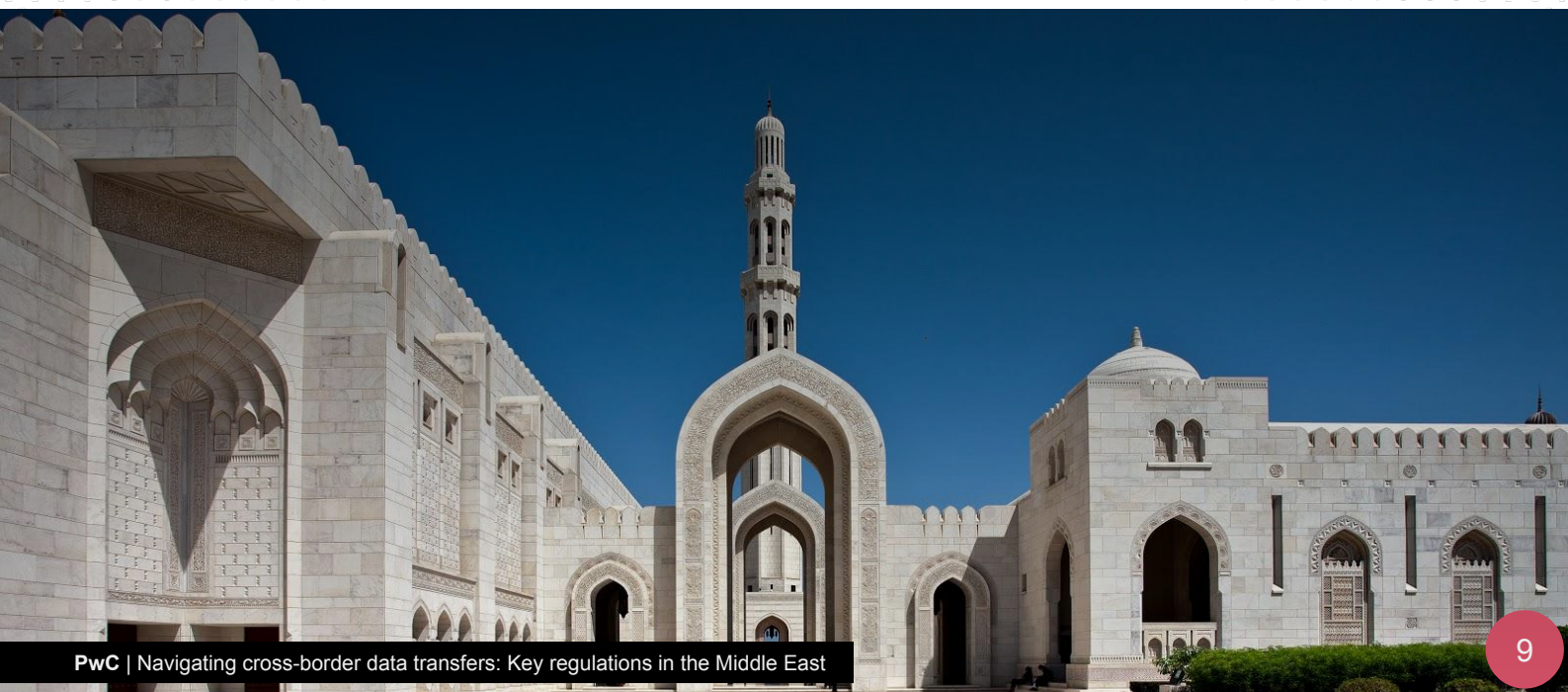
No authorisation from the regulatory authority is required for cross-border transfers.

Key requirements:

- **Explicit consent:** As a general rule, explicit consent of the data subject is the sole lawful basis for processing personal data, including for its cross-border transfer. However, obtaining the consent of the data subject is not necessary if the transfer is performed in an execution of an international agreement to which Oman is a party or if the data is anonymised (Article 37 of the Regulation).
- **Transfer impact assessment:** The controller must conduct an assessment of the level of protection provided by the external processing party, as well as of the risks related to the transfer of personal data. The ministry may request a copy of such an assessment (Article 39, Article 40 of the Regulation).

PwC Middle East key insights

- By providing only one key lawful basis for transfers (subject to two exceptions), the Law and Regulation substantially restrict the transfers of personal data outside its borders.



Kuwait

Key laws and regulations in the personal data protection area

- Data Privacy Protection Regulation No. 26 of 2024 ("**Regulation**") - fully enforceable from February 2025.
- Law No. 20 of 2014 Concerning Electronic Transactions ("**E-Transaction Law**").

Key rules on the cross-border data transfer

Regulatory authority:

Communications and Telecommunications Regulatory Authority (CITRA).

Need for authorisation:

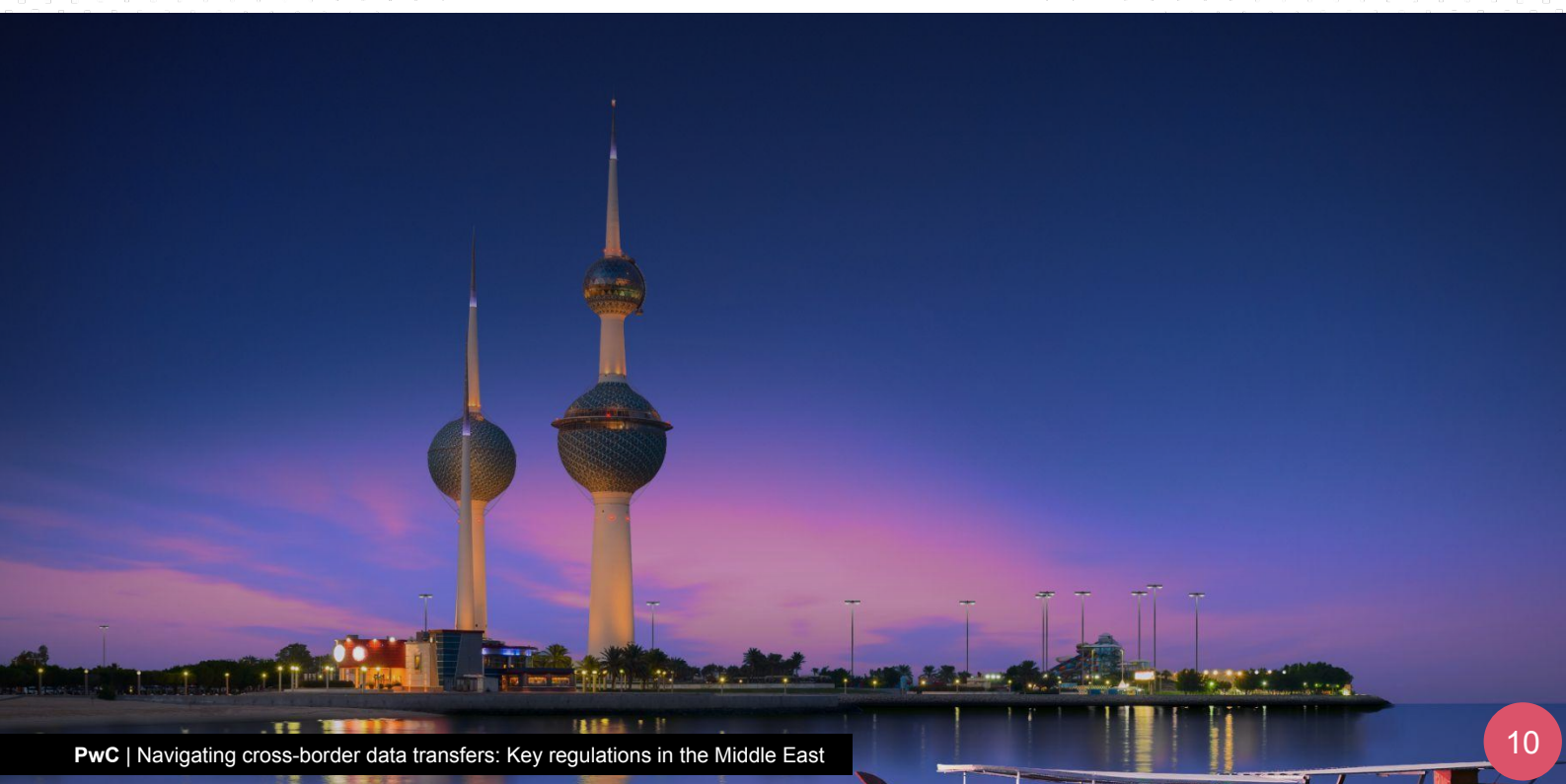
No authorisation from the regulatory authority is required for cross-border transfers.

Key requirements:

- **Scope:** The Regulation generally applies to the use of personal data by service providers who are the entities licensed by CITRA. However, from the definition of "service provider", it is not fully clear if the rules of the Regulation can also apply to any other non-licensed entities that provide content to the general public over the internet.
- **Notification of the data subject:** The service provider must notify the data subject if the service provider intends to transfer the personal data outside of Kuwait (Article 4 of Regulation). This needs to be done in accordance with CITRA's data classification policy.

PwC Middle East key insights

- The Regulation and E-Transaction Law do not provide substantial regulation of cross-border personal data transfers.



Egypt

Key laws and regulations in the personal data protection area

- Personal Data Protection Law No. 151 of 2020 (“**PDPL**”).

Key rules on the cross-border data transfer

Regulatory authority:

Personal Data Protection Centre (“**PDPC**”).

Need for authorisation:

Yes, license or permit is required from PDPC for cross-border data transfers.

Key requirements:

- **Adequate protection:** In addition to the required licence or permit, it must be proved that the recipient country has a level of protection for personal data that is not less than PDPL (Article 14 of the PDPL).
- **Required safeguard:** The personal data could be transferred to the country that does not have an adequate level of protection subject to the explicit consent of the data subject or based on some other lawful bases of data transfer - e.g. vital interests, international judicial cooperation, etc. (Article 15 of the PDPL). However it is not fully clear whether in these cases the authorisation from PDPC will be still required.

PwC Middle East key insights

- The law overall substantially restricts cross-border data transfer.



Lebanon

Key laws and regulations in the personal data protection area

- Law No. 81 of 10 October 2018 on Electronic Transaction and Personal Data (“ETPDL”).

Key rules on the cross-border data transfer

Regulatory authority:

Commission Nationale de la Protection des Données Personnelles (CNPDP).

Need for authorisation:

Yes, authorisation is required in most cases. The ETPDL requires the submission of a permit to the Ministry of Economy and Trade, which must include details about any transfer of personal data outside of Lebanon. Additionally, a license is necessary in certain cases, such as when processing sensitive data (Article 95, Article 96, and Article 97 of the ETPDL).

Key requirements:

- **Exception to the authorisation requirements:** A list of cases in which personal data processing (including transfer) would not require permits or licences is provided in the law (Article 94 of the ETPDL).

PwC Middle East key insights

- The law does not substantially regulate cross-border data transfer.



Jordan

Key laws and regulations in the personal data protection area

- Law No. (24) of 2023, Personal Data Protection Law (“**PDPL**”).

Key rules on the cross-border data transfer

Regulatory authority:

The Personal Data Protection Council (“**Council**”) and an organisational unit under the Ministry of Digital Economy and Entrepreneurship (“**Unit**”).

Need for authorisation:

Authorisation for cross-border data transfers is not required. That said, the PDPL provides the Council with the authority to issue permits for personal data transfers (Article 17 of the PDPL).

Key requirements:

- **Adequate protection requirement:** The transfer of personal data outside Jordan is generally prohibited, unless the data recipient ensures a level of data protection equivalent to that provided by the PDPL (Article 15 of the Law).
- **Transfers to non-adequate countries:** Cross-border data transfers to non-adequate countries are allowed, for instance, for judicial cooperation, medical necessity, and public health reasons, or when explicit consent has been obtained from the data subject after informing them of the insufficient protection (Article 15 of the Law).

PwC Middle East key insights

- It is not fully clear from the PDPL in which cases the cross-border data transfers require permits from the Council.



Tunisia

Key laws and regulations in the personal data protection area

- Act No. 2004-63 of 27 July 2004 on Personal Data Protection (“**Act**”).

Key rules on the cross-border data transfer

Regulatory authority: Instance Nationale de Protection des Données à Caractère Personnel (“**INPDP**”).

Need for authorisation: Yes, any transfer of personal data to a foreign state requires prior authorisation from the INPDP (Article 52 of the Act).

Key requirements:

- **Adequacy of protection:** A transfer can only take place if the foreign state provides an adequate level of protection, considering the type, purpose, and duration of data processing, as well as safety precautions taken (Article 51 of the Act).
- **Express consent:** As a general rule the data transfers require explicit consent, unless the transfers are required for performance of public authorities’ tasks or legal requirements (Article 47 of the Act).

PwC Middle East key insights

- The law overall substantially restricts cross-border data transfers.
- The new personal data protection law is currently in a draft stage. It is expected that the new law will be more aligned with the EU’s General Data Protection Regulation (GDPR).



Morocco

Key laws and regulations in the personal data protection area

- Law No. 09-08 on Protection of Individuals Regarding Processing of Personal Data (“**PIPL**”).
- Executive regulations, Decree No. 2-09-165.

Key rules on the cross-border data transfer

Regulatory authority: Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (“**CNDP**”).

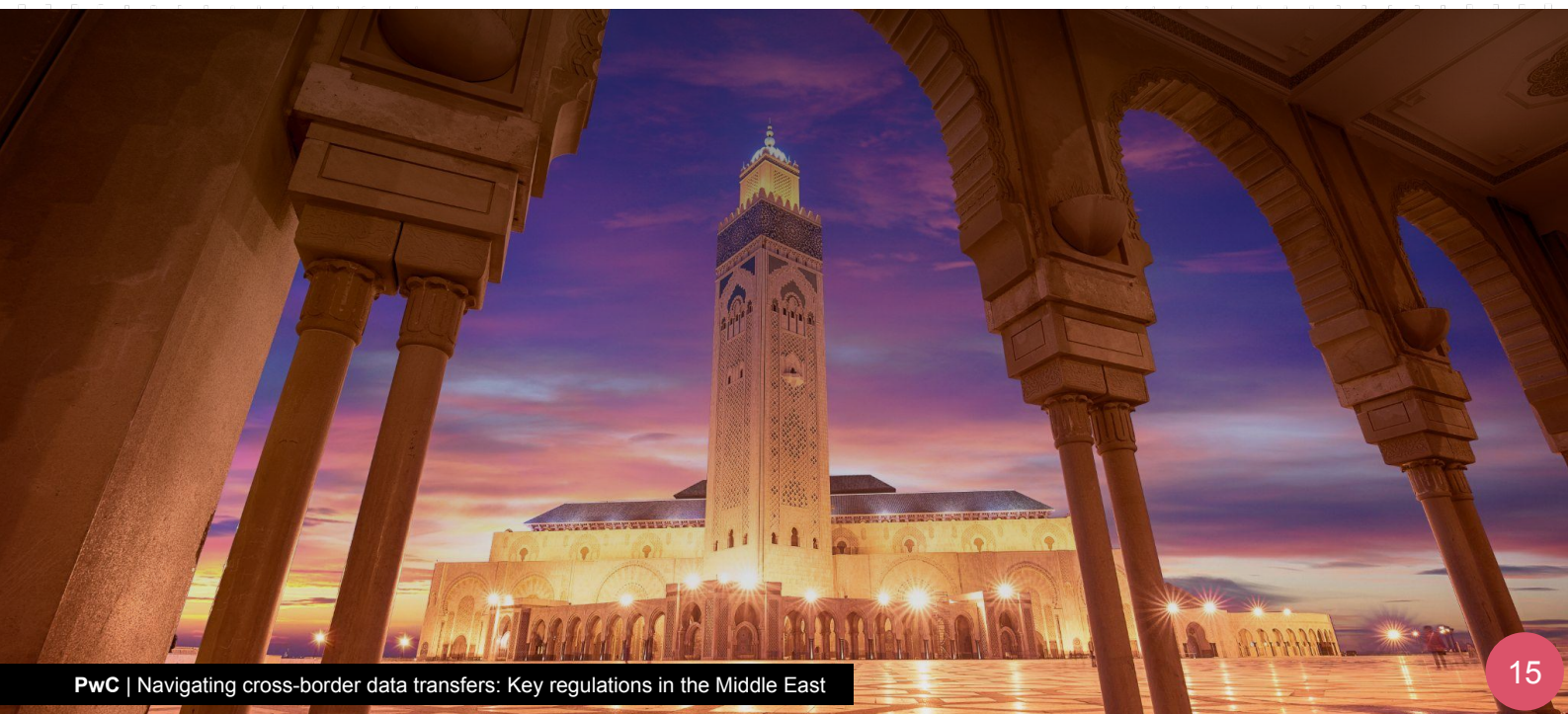
Need for authorisation: Yes, authorisation is required when the personal data is transferred (i) to a country lacking adequate protection or an international agreement with the Kingdom of Morocco; (ii) without the consent of the data subject; and (iii) when none of the cases in which transfers would be necessary (set forth in Article 44 of the PPIPL) are met.

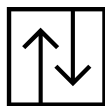
Key requirements:

- **Consent and adequate protection:** Explicit consent of the data subject is required for all data transfers, unless the personal data is transferred to the countries providing adequate protection as determined by the CNDP (Article 43 and Article 44 of the PPIPL).
- **Exemption cases:** Personal data can be transferred without the explicit consent of the data subject in specific cases, for instance for medical needs, performance of legal rights, contractual obligations, judicial cooperation, public interest, or financial transactions (Article 44 of the PPIPL).

PwC Middle East key insights

- It is not fully clear whether in practice transfers of personal data from Morocco to other countries in any case require authorisation by CNDP.





Your path to secure Cross-Border Data Transfers

As cross-border data transfers become increasingly regulated, it is crucial for organisations in the region to ensure compliance. PwC Middle East, with its team of data privacy specialists, is well equipped to assist your organisation on its path to compliance. Our approach to enhancing privacy programmes includes tools and accelerators to facilitate the process; risk analysis and data discovery; gap assessment; building target operating models and programme design; programme implementation, and continuous operations and monitoring. Let us guide you through the intricate and evolving legislation, ensuring that your organisation is compliant with the latest regulations.

To discuss how PwC can support you with personal data protection compliance, please get in touch.



Phil Mennie

Partner, Cybersecurity and Digital Trust

+971 56 369 7736

phil.mennie@pwc.com

[linkedin.com/in/philmennie](https://www.linkedin.com/in/philmennie) @philmennie



Alexander Ladeyshchikov

Manager, Cybersecurity and Digital Trust

+966 56 204 8655

alexander.ladeyshchikov@pwc.com

[linkedin.com/in/alexander-ladeyshchikov-068120122](https://www.linkedin.com/in/alexander-ladeyshchikov-068120122)

About PwC

Established in the Middle East for 40 years, PwC has 22 offices across 12 countries. As a community of solvers, with 8,000 people across the region, we bring the right combination of people, technology and expert capabilities from Strategy, through Advisory and Consulting to Tax and Assurance Services, to solve the region's most pressing challenges (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.

© 2024 PwC. All rights reserved