Monetization of Data: Legal Implications in the UAE and KSA

PwC FinTech Middle East

May 2024

Did you know that you can use data to make money?

Analysing and processing data is the new gold mine for generating revenue.

The global data monetization market is projected to reach an astounding $243.4 Billion by 2027*, with the Middle East region alone is set to contribute $16.793 billion by 2029**.

As businesses unlock the hidden value of data, understanding the legal landscape becomes crucial, especially in regions like the UAE and KSA, where data privacy and data protection is a major concern.

In this article, we provide a high-level overview of the transformative world of data monetization by providing **essential insights** and **practical guidance** for businesses to thrive while **staying compliant** with the **data protections laws** of the UAE and KSA.

Here's what you will discover:

- **What is data monetization?**
- **Balancing profits and privacy concerns**
- **Legal means to monetize data within UAE and KSA.**
- **Best practices for your business.**
- **How we can help you achieve your goals.**

Dive in to learn how to turn data into a powerful asset, unlock new revenue streams, and stay ahead of the competition while navigating the legal intricacies of data monetization in the UAE and KSA.

What is Data Monetization?

Data monetization refers to the process of using data to generate economic value. This could be through direct means, such as selling the data itself or through indirect methods, which involve extracting insights from the data that can lead to improved decision-making and strategic business moves.

The innovative use of data is transforming how companies operate, offering them new revenue streams and a competitive edge in the market. In 2020, the market for data monetization was valued at USD 2.1 billion, and is expected to grow at an impressive compound annual growth rate (CAGR) of 22.1% between 2021 to 2030.

The Growth of Data Sector in the UAE and KSA

The widespread use of internet and social media generates substantial data which is being monetized innovatively to generate new revenue streams.

The statistics below highlight the immense potential for data monetization in the region, though it underscores the necessity for stringent data protection to prevent misuse of personal information.

UAE***

In 2024, the UAE achieved a 99% internet access rate

9.46 million users

High social media engagement exceeding the population by 12%

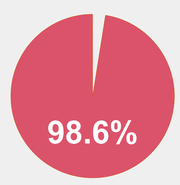
10.73 million users

219.4% of the population, indicating many individuals with multiple subscriptions.

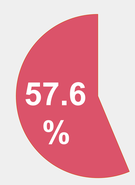
20.96 million connections

KSA****

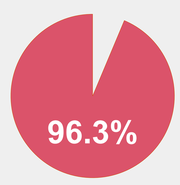
Internet penetration stands at an impressive 98.6%.



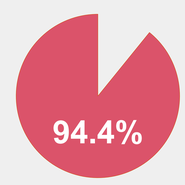
Cloud storage services are used by 57.6% of the population.



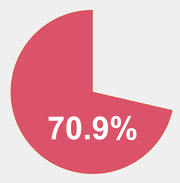
A majority of the population utilizing online government services 96.3%



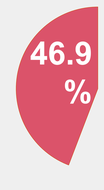
E-commerce is also thriving, with 94.4% patronizing local online stores



70.9% of the population uses banking electronically



46.9% of the population is shopping internationally.



* New Data Economy Report, Dubai Economy, 2021.
** Middle East and Africa Data Monetization Market - Forecasts from 2024 to 2029, 2024.
**** The Communications, Space, and Technology Commission,Saudi internet, 2022.

Legal Frameworks in the UAE

Aligning with international best practices such as the GDPR, the UAE issued Federal Decree Law No. 45 of 2021 concerning the Protection of Personal Data ("**UAE PDPL**") as the primary legal instrument governing data privacy, particularly in relation to data monetization. The UAE PDPL applies to the processing of personal data by electronic or other means, by any natural or legal person, inside or outside the UAE, as long as the data subject resides or has a place of business in the UAE, or the processing affects the data subject's rights or obligations in the UAE.

The UAE PDPL defines personal data as data related to a specific or identifiable person, including sensitive and biometric data. The law also defines the controller as the one who determines the method and purpose of processing, and the processor as the one who processes data for the controller.

The UAE has various other policies and strategies for data protection, such as the Consumer Protection Law (Federal Law No. 15 of 2020), which includes provisions for protecting consumer data, prohibiting the misuse of consumer data for marketing without consent. Similarly, the DIFC Data Protection Law, and the ADGM regulations also set data protection standards and consumer rights.

Thus, the UAE has made significant strides in the field of data privacy in the UAE, and it will have implications for any business entity that processes personal data and engages in data monetization.

The UAE PDPL sets out the following key requirements for processing personal data

Consent

- You can process personal data with the consent of your customer, unless the processing falls under one of the exceptions specified in the law, such as public interest, legal claim, contractual obligation, or public health.
- The consent must be specific, clear, unambiguous, and easily accessible, and the customer has the right to withdraw their consent at any time.

Rights

- Your customer has the right to receive information, the right to request transfer, correction, erasure, or restriction of their personal data, or to object to or stop the processing of their personal data.
- You, as the controller must provide clear and appropriate ways for the data subject to contact the controller and to exercise their rights.

Controls

- You must process data in a fair, transparent, and lawful manner, and must be limited to what is necessary for the purpose of processing.
- You, as the controller, and your processor must take appropriate technical and organizational measures to ensure the protection of personal data.

Data Protection Officer (DPO)

- You, as the controller and the processor must appoint a DPO, who has sufficient skills and knowledge of the personal data protection law if the processing involves a high-level risk, a systematic and comprehensive assessment, or a large volume of sensitive personal data.
- The DPO is responsible for ensuring the compliance of the controller and the processor with the UAE PDPL.

Cross-Border Transfer and Sharing

- The law also regulates the cross-border transfer and sharing of personal data for processing purposes, which is subject to certain conditions and approval of the UAE Data Office.
- You can transfer personal data to entities or countries that have adequate legislation on personal data protection, or that are parties to bilateral or multilateral agreements on the same matter.

Examples

An e-commerce platform that onboards customers wishes to sell the personal data to third-party marketing agencies for targetted ads. In such cases, the company must obtain clear, written consent to do so from the customers through their terms of use.

Taking the same example, a customer of the e-commerce company wishes to restrict use of his personal data a for marketing purposes. Once the customer makes such a request, the e-commerce company will have to comply with it under the UAE PDPL.

A data processing company must have sufficient policies, procedures and security measures (such as secured servers with firewalls) to protect and safeguard customers' personal data.

A credit rating company must appoint a qualified DPO in compliance with the UAE PDPL. The DPO bears the primary responsibility of overseeing compliance with the UAE PDPL, training employees, developing policies and internal procedures and assessing risk from a data protection perspective.

A company in UAE that wishes to transfer data to its parent company in UK should have intercompany data transfer agreements that sets out the roles, responsibilities, liabilities and obligations in accordance with the laws.

Legal Frameworks in KSA

Personal data protection laws in the Kingdom of Saudi Arabia (KSA) have recently undergone significant changes, with the enactment of the Personal Data Protection Law (PDPL) and its Implementing Regulation (IR).

These laws impose new obligations and responsibilities on business entities that process personal data and monetize it, such as direct marketing, credit reporting, or data analytics.

Apart from the above, the PDPL and IR impose obligations and responsibilities on the data controllers similar to that of the UAE PDPL Law.

Saudi Arabia also has other laws that protect personal data, such as the E-Commerce Law which prohibits unauthorized use or disclosure of consumer's personal data and requires the protection of customer data and consent for its use in marketing.

Similar to that of the UAE PDPL Law, and in alignment with the GDPR, the PDPL and IR of KSA set out the key requirements of processing data which are as follows:

Consent and Exceptions

- Data controllers must obtain data subjects' consent for processing personal data, with exceptions (i.e., legal or contractual requirements, vital / legitimate interests, etc.).
- Consent should be voluntary, clear, specific, documented, and retractable. Sensitive data, credit data, or automated decision-making require explicit consent.

Rights

- Data subjects have the right to be informed, a right to access, correct, and request the destruction of their personal data held by data controllers.
- Data controllers must act on data subject requests within 30 days, verify their identity, and document the request.
- Data controllers can refuse requests that are repetitive, unfounded, or require disproportionate effort.

Collection and Processing

- Data controllers must collect only the minimum amount of personal data necessary for the processing purposes and destroy it when it is no longer needed.
- Data controllers must inform data subjects of the data retention period and the legal basis for it.

Disclosure and Transfer

- The PDPL and the IR restrict the disclosure and transfer of personal data to third parties, except under specific conditions, such as consent or public interest.
- Transfer of personal data outside the KSA is subject to conditions ensuring adequate protection and is limited to the minimum necessary data.

Data Protection and Breach Notification

- Data controllers must implement measures to ensure the security and privacy of personal data and prevent unauthorized access, disclosure, or alteration.
- Data controllers must notify the Competent Authority and the data subject of any data breach that could harm the personal data or the data subject within 72 hours of becoming aware of it.

Examples

A data analytics firm collecting and processing personal data for client insights must obtain specific consent from data subjects (unless exempted). Consent should be specific to processing scope and purpose, and must be withdrawable. Explicit consent is necessary for processing sensitive data or making automated decisions.

A direct marketing company that sends promotional messages to customers based on their personal data must inform them about the legal basis and purpose of data collection, and provide them with a method to access, correct, or delete their personal data.

A credit reporting company that collects and processes personal data from data subjects and third parties to generate credit scores and reports must ensure that the data collection and processing are necessary, proportionate, and lawful, and that the data subjects are informed and consent to the processing.

A data monetization company that sells or shares personal data with other entities for commercial purposes must obtain consent from the data subjects before disclosing or transferring their data, unless it falls under one of the exceptions.

A data controller that suffers a cyberattack that exposes personal data must report the incident and take steps to mitigate the damage.

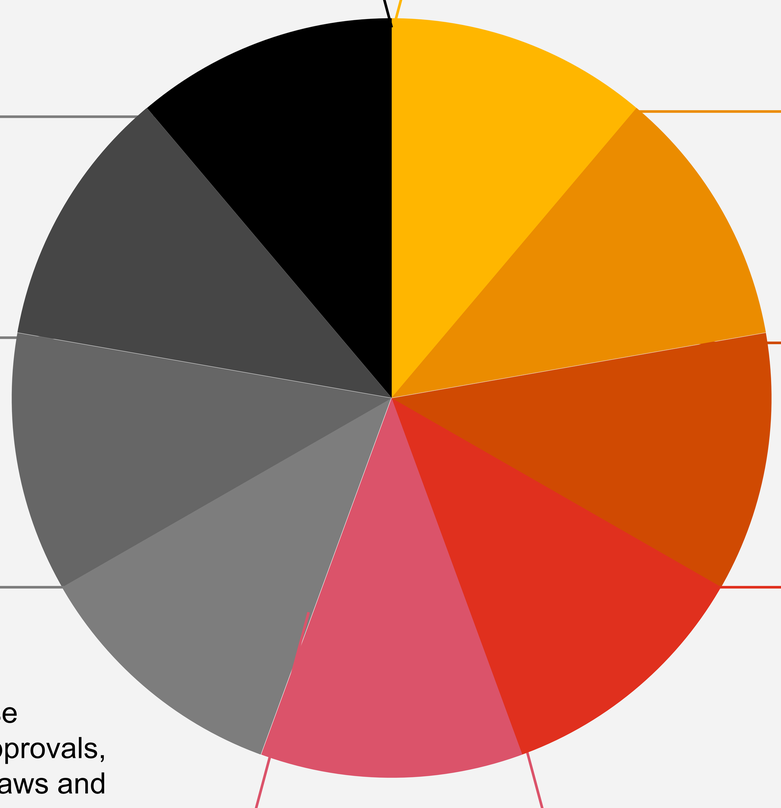
Best Practices for your Business

Data monetization is a lucrative and innovative trend that can offer business entities new opportunities and competitive advantages in the UAE and KSA. However, it also entails legal obligations and responsibilities to protect the personal data of individuals from misuse or harm.

As such, we recommend following these best practices for processing data and monetizing it:

DPO Surveillance
Appoint a data protection officer (DPO) who has sufficient skills and knowledge of the data protection laws and regulations, and who can oversee the compliance of the data controller and processor and their obligations.

Outsourcing Practices
Vet third-party vendors to ensure they have strong data protection measures, create contracts that clearly outline responsibilities and liabilities for data breaches, and continuously monitor and audit their compliance with data protection standards.



Secure Transfer of Data
When you are transferring or sharing personal data across borders, ensure that the recipient jurisdiction or entity has adequate data protection standards and/or safeguards.

Unwavering Consent
Obtain clear and specific consent from customers for the collection, use, and transfer of their personal data, unless there is a valid legal basis for processing without consent.

Policies and Procedures
Develop and enforce data protection policies that comply with laws, regularly train employees and audit practices to ensure compliance, and create a clear plan for swift and effective response to data breaches.

Controls and Safeguards
Implement appropriate technical and organizational measures to ensure the security and confidentiality of personal data, and prevent unauthorized access, disclosure, or breach.

Intra-group Transfer
Establish intra-group agreements that clearly define roles, responsibilities, and liabilities for data transfers, ensure these agreements meet legal standards and receive necessary approvals, and regularly update them to stay compliant with changing laws and practices.

Limited Collection
Limit the collection and processing of personal data to what is necessary and relevant for the purpose of data monetization, and delete or anonymize the data when it is no longer needed.

Clear Purpose
Clearly define the purpose and requirements for collecting personal data from customers.

How We Can Help

With PwC's expertise, you can confidently monetize data while staying fully compliant with all legal requirements.

PwC offers expert guidance on compliance with UAE and KSA data protection laws. Our team of experienced lawyers and professionals provides:

Expert legal advice	We provide expert legal advice and tailored solutions to help your business navigate the complexities of data protection regulations.
Policy Development and Implemmention	We can also develop and implement robust data protection policies, conducting regular training sessions and audits, and establishing effective incident response plans.
Inter-group Agreements	We can create detailed inter-group agreements for secure data transfers and ensure these agreements meet legal standards.
Compliance Support	We support in vetting third-party vendors, creating legally enforceable contracts, and monitoring their compliance with data protection standards.

Get in touch to find out more

Shayan Dasgupta
Legal - Fintech
Manager (UAE)
E: shayan.dasgupta@pwc.com

Hussein Kanji
Legal - Fintech
Manager (UAE)
E: hussein.kanji@pwc.com

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with over 328,000 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 24 offices across 12 countries in the region with around 10,300 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.