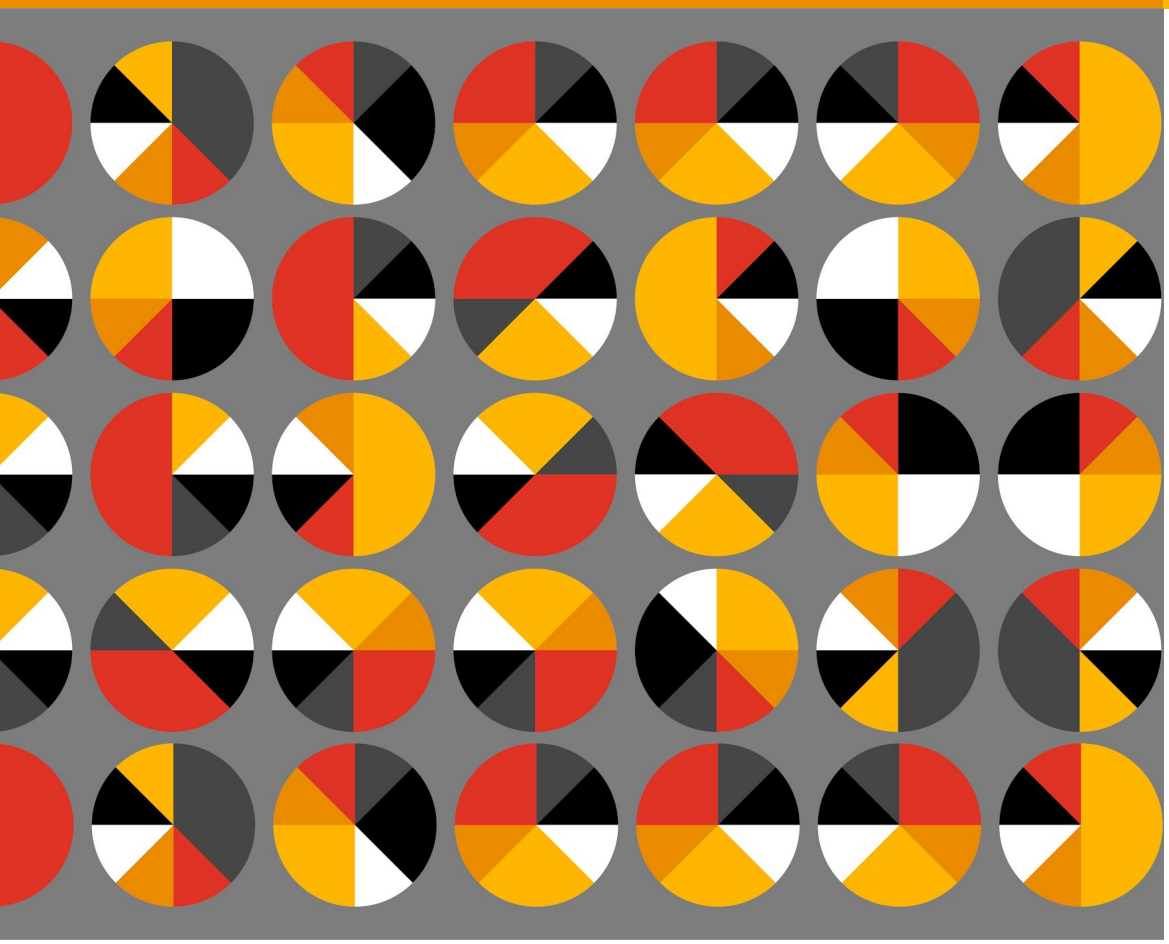
Saudi Arabia: Data Privacy Landscape

November 2019



Insights
Tax and Legal Services
PwC Middle East

pwc

In brief

Whilst there is currently no dedicated data protection legislation in force in the Kingdom of Saudi Arabia (KSA), the increase in global data protection laws and market awareness of individual data protection rights and ownership are giving rise to new challenges affecting businesses in KSA and indeed globally. Consistent with a lot of jurisdictions in the region, the privacy of an individual and the safeguarding of their personal data are provided under general provisions of KSA law, rather than ones specifically focused on the issue of "data privacy" or "data protection".

As we will see however, things are changing in KSA with new laws emerging aimed at imposing strict obligations on businesses in KSA in relation to how, why and when personal data can be collected, used and stored.

In detail

Sharia Law

Given the absence of specific legislation on data protection, the courts of KSA have historically dealt with data privacy issues under general Sharia principles - the collection of general principles derived primarily from the Holy Qur'an and Sunnah (the witnessed sayings and actions of the Prophet Muhammad) which form the basis of the legal system in KSA. Under the KSA Basic Law of Governance, the privacy rights of individuals are protected in accordance with Sharia law to the extent that telegraphic, postal, telephone and other means of communications are safeguarded and cannot be confiscated, delayed, read or breached.

Electronic Commerce Law

In October 2019, Royal Decree No. M/126, the E-Commerce Law, came into force. The law applies to e-commerce service providers, including those who are located outside of KSA, who offer goods/services to customers based in KSA. Like the EU General Data Protection Regulation (GDPR), the law will have extraterritorial effect, applying, for example, to websites in the UAE that sell goods or services to customers in KSA.

The E-Commerce Law focuses on regulating e-commerce business practices requiring increased transparency and consumer protection, with the goal of enhancing trust in online transactions. The law also contains provisions aimed at protecting the personal data of e-commerce customers. Specifically, the law specifies that service providers will be responsible for protecting the personal data of customers in their possession or 'under their control'. 'Control' in a data protection context exists where an organisation can make decisions concerning that personal data, such as why to collect it in the first place, what to do with it, how long to keep it, and who to share it with. A service provider may still have 'control' of personal data where it passes the data on to a third party as part of an outsourcing or other arrangement.

Data retention is also a focus point, with provisions stating that service providers must not retain personal data for longer than is required for the purposes of the transaction. This mirrors the '*storage limitation principle*' set out in the GDPR, namely that personal data must not be kept for longer than is necessary for the purpose for which the data was collected. In practice, this means that service providers should retain personal data no longer than it is needed for their objective business needs and should implement and follow a data retention policy setting out such time limits.

The KSA E-Commerce Law also prohibits service providers from using customers' personal data for 'unlicensed or unauthorised' purposes, and from disclosing personal data to third parties without the customer's consent.

There are no provisions governing the transfer of personal data outside of KSA, but with implementing regulations pending and expected after the law comes into force, it is likely that these will cover this issue.

Cloud Computing Framework

The KSA Cloud Computing Regulatory Framework (CCF) is based on international best practices and governs the rights and obligations of cloud service providers (CSPs), individual customers, government entities and businesses. The CCF is one of only a few examples of cloud-specific regulatory frameworks around the world and includes principles of data protection. Some of the provisions, such as security breach notification, are in line with the approach taken in the EU, while others, such as the requirement to register with the Communications and Information Technology Commission (CITC) content classification, are specific to KSA. Some of the most important features of the CCF from a data protection perspective, are the cloud security requirements CSPs must adhere to - cloud customer information can be subject to different levels of information security, depending on the required level of preservation of the information's confidentiality, integrity, and availability. CSPs must also inform any cloud customer, upon request, of the information security features offered by the CSP or applied to the cloud customer's information.

Security Level	Categories of Customer Data
Level 1	Non-sensitive customer content of individuals, or private sector companies, not subject to any sector-specific restrictions on the outsourcing of data.
Level 2	Sensitive customer content of individuals, private sector companies, not subject to any sector-specific restrictions on the outsourcing of data; and non-sensitive customer content from public authorities.
Level 3	Any customer content from private sector-regulated industries, subject to Level 3 categorisation under sector-specific rules or regulatory decision; and sensitive customer content from public authorities.
Level 4	Highly sensitive or secret customer content belonging to relevant governmental agencies or institutions.

The CCF also contains several statutory presumptions about how such customer information should be classified from an information security standpoint (unless requested otherwise). These information security presumptions (by category of cloud customer) are:

- for natural persons with a residence in KSA: Level 1 treatment of Customer Content;
- for private sector legal persons, such as companies incorporated or with a customer address in KSA: Level 2 treatment of Customer Content;
- for any government or state services or agencies: Level 3 treatment of Customer Content; and
- for all other categories: Level 1 treatment of Customer Content.

The CCF also sets out breach notification requirements (to both the cloud customer and the CITC in specified circumstances), limited data subject rights, and restrictions around third-party data sharing, including specifically on transferring certain data outside KSA.

Cloud customers must ensure that no Level 3 Customer Content is transferred outside KSA, for whatever purpose and in whatever format, whether permanently or temporarily (e.g. for caching, redundancy or similar purposes), unless this is expressly allowed under KSA law. Cloud customers must also not transfer, store or process Level 3 Customer Content to or in, any public, community or hybrid cloud unless and for as long as the CSP is validly registered with the CITC. CSPs must also inform their cloud customers in advance whether their Customer Content will be transferred, stored or processed outside KSA, permanently or temporarily.

The CCF is likely to be just one of many first steps toward a clearer and more transparent regulatory approach in the information communication technology sector in KSA, especially as KSA looks towards its ambitious 2030 vision.

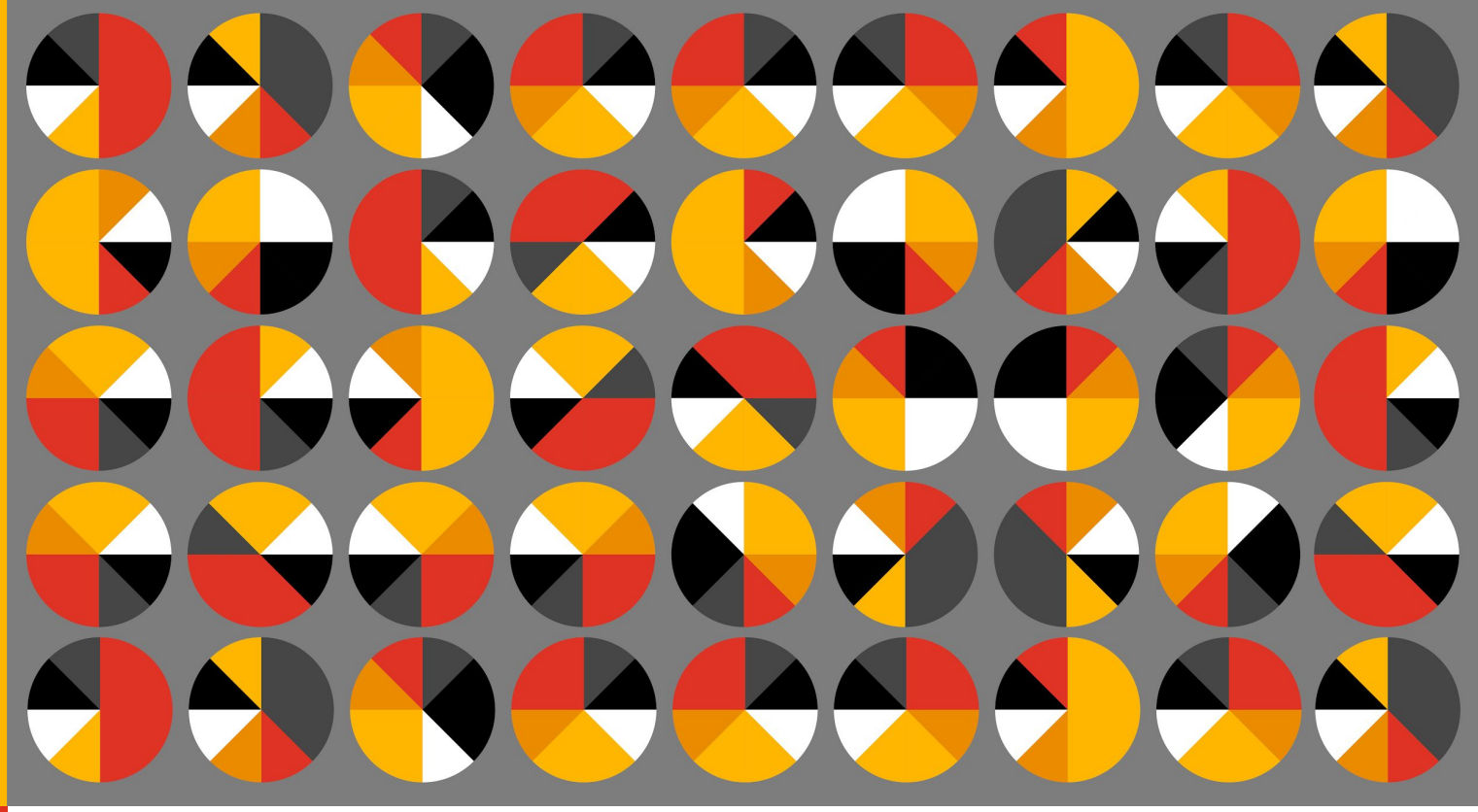
Internet of Things (IoT) Regulatory Framework

Published by the Communications and Information Technology Commission (CITC), the IoT Regulatory Framework regulates all use of IoT services in KSA. The Framework requires providers of IoT services to comply with 'data security, privacy and protection requirements'. The Framework goes on to state that IoT providers and implementers must 'comply with all the existing or future published laws, regulations and requirements… concerning data management including security, privacy and protection'. The Framework therefore envisages that specific data protection laws may be enacted in the Kingdom at some point (indeed, as we will see below, these are already in development). Drawing on the generally accepted data protection concepts and principles therefore, it is likely that IoT service providers will be required, amongst other things, to:

- only collect personal data for specified and lawful purposes and not use that information for any reason that would be incompatible with those purposes (purpose limitation);
- only collect as much data from users as is actually needed in order to achieve the above purposes and no more (data minimisation);
- retain this data only for so long as it is actually needed in order to achieve the above purposes and no longer unless the law requires otherwise (storage limitation);
- deploy appropriate data security measures in order to guard against unauthorised access, loss, destruction, disclosure etc. of the data.

Consistent with several emerging laws in the region, including the CCF, the Framework also refers to data localisation rules, requiring all servers used in providing IoT services, all IoT network components, devices and hosts of the data, as 'all data', to be kept inside KSA. The data from IoT devices and machines must also be kept for a duration of not less than 12 months, 'or any other duration specified by the CITC'.

Finally, the Framework also contains a requirement similar to the right to be informed under the GDPR. IoT service providers must make end users aware of 'the importance of the network and data security' and must 'provide the user with recommendations to protect the data'. This perhaps suggests that IoT service providers will be required to make this information available to users in a form similar to a privacy notice. More details are can be expected in future laws and regulations.



Electronic Transactions Law

Although there is no specific mention of personal data, the Electronic Transactions Law (Royal Decree No M/18) imposes certain obligations on internet service providers (ISPs), stating that ISPs and their staff must maintain the confidentiality of information obtained in the course of business. This would, presumably, include all personal data collected. The law also states that personal data must only be obtained, whether directly or indirectly, with the individual's written consent. The law therefore provides limited protection for personal data, however only in the context of electronic transactions.

Anti-Cyber Crime Law

The Anti-Cyber Crime Law (Royal Decree No M/17) aims to ensure information security, protection of rights pertaining to the legitimate use of computers and information networks, protection of public interest, morals and protection of the national economy. The law contains limited provisions in relation to cyber data protection.

The law makes it an offence to access the computer of another for the purpose of deleting, destroying, altering or redistributing its information, to access the bank or credit information of another, and to interrupt data that is transmitted through a computer or information network. Additionally, the law stipulates that an individual's consent must be obtained in order to process their personal data, including disclosing any documents obtained by such processing.

Applicability of the GDPR

From 25 May 2018, companies in KSA that process personal data of EU-based data subjects in the context of the activities of a European establishment, offer goods or services to, or monitor the behaviour of, EU-based data subjects may need to comply with the GDPR. Subject to certain exceptions, businesses in KSA that fall within the scope of the GDPR must appoint an EU representative, located in one of the European countries of the individuals who are offered products, or subject to behavioural monitoring. The representative acts on behalf of the KSA company and may be addressed by any EU data protection supervisory authority and data subjects.

The takeaway

The GDPR has undoubtedly been a catalyst and harbinger of change in setting the baseline standards of personal data privacy across the world. Although there is currently no specific data protection legislation in place in KSA, personal data and privacy are somewhat protected in other sectoral laws, particularly in the context of technology and electronic communications.

Looking to the future, recent media reports suggest that a new "Freedom of Information and Protection of Private Data Law" is under review by the formal advisory body of KSA, the Shura Council. It has been reported that the law will be modelled on, and incorporate familiar concepts from, other international privacy frameworks, such as the 1995 EU Data Protection Directive (and by extension the GDPR) and will mandate that any party who processes personal data must adhere to the principles of transparency, fairness and accountability.

www.pwc.com/me

Let's talk

For a deeper discussion of how this issue might affect your business, please contact:

Matt White
Partner, Head of Digital Trust
+971 56 113 4205
matt.white@pwc.com

Darren Harris
Head of Legal Services
+971 56 418 9768
darren.harris@pwc.com

Phil Mennie
Partner, Digital Trust
+971 56 369 7736
phil.mennie@pwc.com

Richard Chudzynski
Legal Data Privacy Leader
+971 56 417 6591
richard.chudzynski@pwc.com