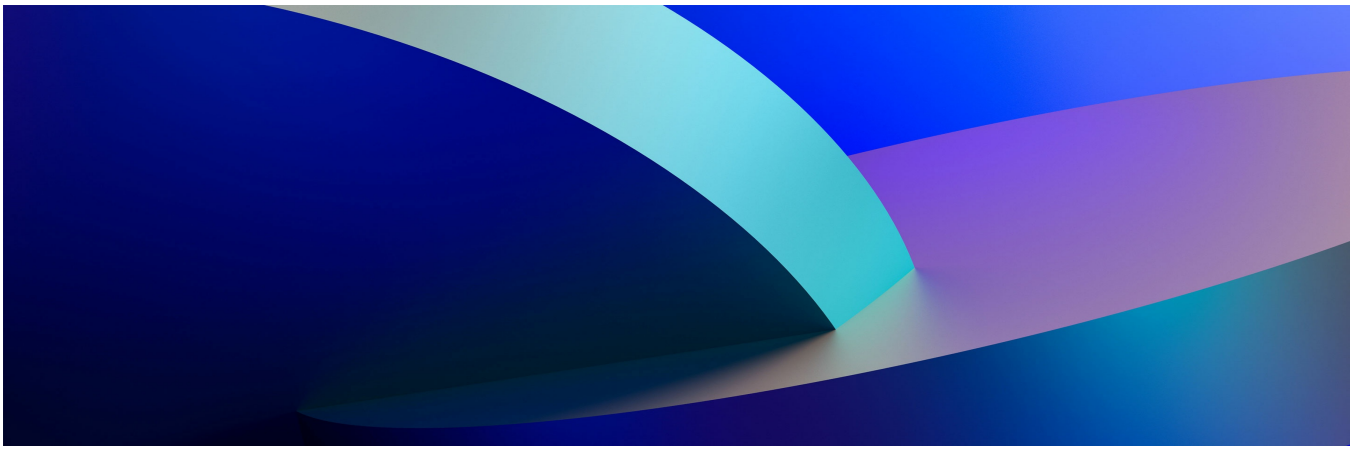

Data protection and cybersecurity laws in Saudi Arabia

Data protection

1. Local data protection laws and scope

Royal Decree M/19 of 9/2/1443H (16 September 2021) approving Resolution No. 98 dated 7/2/1443H (14 September 2021) The Personal Data Protection Law ("**PDPL**") is the main data protection law in KSA. **PDPL takes effect on 23 March 2022 and there is a compliance grace-period of one year until 23 March 2023**. Further implementing regulations are due to be published in advance of the effective date.
There are also other sector specific laws and other mandatory documents which address data protection.

Cybersecurity Law

The Anti-Cybercrimes Law of 2017 (the "**Cybersecurity Law**") is a general law that applies across the board and addresses data protection in the context cybercrimes.

National Data Regulations

The National Data Governance Interim Regulations of 2020 (the "**National Data Regulations**") issued by the National Data Management Office deal mainly with government-related data. Part 5 of the National Data Regulations, however, deals with personal data protection and is stated to apply to all entities in KSA that process personal data in whole or part, as well as all entities outside KSA that process personal data related to individuals residing in KSA. The legal status of the National Data Regulations remains slightly unclear at the time of writing and it is not clear if they are being actively enforced. No sanctions for breach are specified, which is unusual for a law which is intended to be enforced. Clearly the potential scope of Part 5 is very extensive and, on the face of it, would catch numerous businesses with no local presence in the Kingdom, such as cloud service providers. Now that the PDPL has been published, we assume that the National Data Regulations are not intended to apply to private businesses in KSA.

Telecommunication and Internet of Things

The Implementing Regulations of the Telecom Law of 2002.

General Principle for Personal Data Protection of 2020 ("**Telecom Data Protection Principles**") covers data protection in the telecommunications, information technology and postal sectors.

Process of Launching Services or Products Based on Users' Personal Data, or Sharing Personal Data of 2020 covers the launching of products in the telecommunications, information technology and postal sectors based on customers' personal data.

The telecommunications regulator, the Communications & Information Technology Commission (CITC), has also published an IoT Regulatory Framework, (IoT RF) regulating the provision of internet-of-things services in the Kingdom. The IoT RF is issued pursuant to the Telecommunications Law.

Cloud services

The Cloud Computing Regulatory Framework (the "**Cloud Framework**") covers data protection of customers of cloud service providers.

Ecommerce

The Ecommerce Law of 2019 and its Implementing Regulations of 2020 cover data protection of customers in the ecommerce business.

Medical

The Medical Practitioners' Law of 2005 also deals with the safeguarding of information obtained during medical practice, which would include their personal data.

2. Data protection authority

Saudi Data and Artificial Intelligence Authority ("**SDAIA**") is the regulator for the initial two years of PDPL. The PDPL anticipates that responsibility will be transferred to the National Data Management Office ("**NDMO**") in due course, but does not commit to this happening. SDAIA and NDMO shall collectively be referred to as the "**Authority**".

- Communication & Information Technology Commission ("**CITC**"): www.citc.gov.sa
- Ministry of Commerce: www.mc.gov.sa
- Saudi Public Prosecution
- Saudi Authority for Data and Artificial Intelligence
- National Data Management Office

3. Anticipated changes to local laws

Implementing regulations are expected to the PDPL.

The National Data Governance Interim Regulations being a new regulation, it is not clear how it will be implemented.

4. Sanctions & non-compliance

Administrative sanctions:

PDPL

There are fines of up to three million Saudi Riyals (SAR 3,000,000) (approximately USD 800,000) for disclosure or publication of sensitive data in breach of PDPL and of up to one million Saudi Riyals (SAR 1,000,000) (approx. USD 266,539) for breaches of data transfer rules. The PDPL also introduces a general maximum fine of five million Saudi Riyals (SAR 3,000,000) (approximately USD 1,332,697) for other violations of the PDPL with the prospect of this being doubled for repeat offenders.

Cybersecurity Law

The Cybercrimes Law imposes a penalty of up to SAR 3m (USD 800,000) for the offence of unauthorised access to, amongst others, destroy, leak or redistribute private data.

Telecommunication and Cloud Services

CITC may impose a fine of up to SAR 25m (USD 6.666m).

Internet of Things

No specific sanctions are set out in the IoT RF but as it is issued pursuant to powers and duties under the Telecommunications Law, the CITC may treat breach of the IoT RF as a breach of the Telecommunications Law.

Ecommerce

The Ecommerce Law imposes a penalty of up to SAR 1m (USD 266,630). Also, the ecommerce business may be suspended or closed, and the internet shop may be blocked, partially or completely, temporarily or permanently.

Criminal sanctions:

PDPL
The PDPL imposes prison terms of max. 2 years where sensitive data are disclosed or published contrary to the PDPL and of max. 1 year for a breach of cross-border data transfer rules.

Cybersecurity Law

The Cybercrimes Law provides for imprisonment of up to four years for the offence of unauthorised access to, amongst others, destroy, leak or redistribute private data.

Others:

A data subject may also make a claim to the courts for damages.

5. Registration / notification / authorisation

PDPL
Article 33 of the PDPL provides that the Authority shall be responsible for issuing licences to commercial, professional or non-profit businesses under the PDPL, however it does not expressly state what, if any, additional licences a business will need to obtain in order to process personal data. Non-KSA based data processing entities which process personal data related to individuals residing in KSA will also have to appoint a representative in KSA, licensed by the Authority, to carry out its obligations under the law. The Council of Ministers resolution which promulgates the PDPL allows the Authority to delay the implementation of Article 33 for up to five years and we expect the implementing regulations which are yet to be published will also deal with this.

Please note sector specific approvals, licenses or registrations, if any, will apply for carrying out the respective economic activities in that sector.

6. Main obligations and processing requirements

PDPL
The PDPL introduces GDPR-style processing obligations. Personal data must be processed on a lawful basis prescribed in the law such as consent or performance of a contract. There are also accountability obligations for controllers similar to the GDPR. There is no “legitimate interests” basis for processing.

Cybersecurity Law

Unauthorised access to private data is prohibited. Accordingly, consent of the individual to whom the personal data belongs should sought before collection or processing.

National Data Regulations

The National Data Regulations sets out principles for dealing with personal data, which include: the purpose of collection of personal data should be known, the data subject's consent should be sought for collection and processing, collection of personal data shall be limited to what is necessary for the purpose, personal data should be used for the agreed purpose only, and data shall be protected against breach.

Telecommunication

The Implementing Regulations of the Telecom Law of 2002 requires service providers to protect the personal information of their customers. Further, the Telecom Data Protection Principles require service providers to comply with the following principles:

- process customers' personal data in a lawful and transparent manner;
- process customers' personal data for specified and clear purposes;
- collect customers' personal data that is necessary for the purposes of the processing;
- not keep customers' personal data in a form that allows identification of the customer for longer than the period necessary to achieve the purposes of processing;
- secure customers' personal data to ensure its privacy and prevent unauthorised access, breach, tampering or misuse.

Internet of Things

The IoT RF contains some basic provisions requiring equipment to comply with mandated standards and for the IoT system to be capable of allowing interrogation of data processed over it for not less than 12 months after the date of creation.

Cloud Services

The Cloud Framework prohibits cloud service providers from (i) providing to any third party any subscriber content or subscriber data; and (ii) processing or using subscriber content or subscriber data for purposes other than those permitted by the cloud subscriber; except where (a) the same is required under KSA laws; or (b) the subscriber's data is of non-governmental nature and is not received from any government entity, and the relevant cloud customer has given their express prior consent (whether in an opt-in or opt-out form).

The provisions of the Telecom Data Protection Principles will apply to cloud service providers in addition to the Cloud Framework.

Ecommerce

The Ecommerce Law requires a service provider to only retain a customer's personal data or electronic communications for the period required by the nature of the electronic transaction, unless a different period is agreed upon.

A service provider is responsible for protecting customers electronic communications or personal data in its possession or in the possession of the entities or agents that it deals with, and is prohibited from using customers' personal data or electronic communications for unauthorised or impermissible purposes and from disclosing the same to third parties, whether against or for no consideration, unless the consumer consents to such disclosure or the same is required by law.

Financial

Financial institutions licensed by the Saudi Central Bank are required to protect their customers' personal data.

Medical

Medical practitioners are prohibited from disclosing any personal data of their patients without the prior consent of their patients.

7. Data subject rights

PDPL
The PDPL confers data rights similar to those contained under GDPR. These rights include the right to be informed about how personal data are processed, obtain access to personal data and the right to request correction and deletion of personal data. Response times for dealing with requests shall be specified in the not yet published implementing regulations of the PDPL.

National Data Regulations

The National Data Regulations prohibit collecting, processing or sharing personal data with third parties without the consent of data subjects. Customers may withdraw such consent at any time. Customers may withdraw such consent at any time unless otherwise required by law. As noted previously, we consider that the PDPL effectively renders these regulations obsolete for private business and that they are effectively a guideline for the public sector.

Telecommunication

The Telecom Data Protection Principles prohibit collecting and processing, or sharing with third parties, customers' personal data without their explicit consent. Customers may withdraw such consent at any time except as otherwise required by law.

Customers should also be enabled to view or be given access to the privacy policy prior to processing their personal data.

Customers should also be enabled to access, correct (amend) and obtain their personal data being processed by the service providers.

Cloud Services

Cloud service providers are required to grant subscribers the right and technical capability to access, verify, correct or delete their subscriber data in a manner that does not contradict the instructions of the National Data Management Office.

8. Processing by third parties

PDPL
Article 15 of the PDPL specifies the limited circumstances in which personal data may be disclosed to third parties. For most businesses, data subject consent to disclosure appears to be the only available option.

Further, the collector of the Ecommerce Law and the Telecom Data Protection Principles provide that the entity collecting data from customers will be responsible for the protection of data, even if it is processed by third parties.

9. Transfers out of country

PDPL

Article 29 of the PDPL prohibits the transfer or disclosure of personal data outside of KSA except in very limited circumstances. These limited circumstances include where the transfer or disclosure is:

- absolutely necessary to preserve the life or vital interest of the data owner outside KSA or to prevent, diagnose or treat infections; or
- in implementation of an obligation under a convention to which KSA is party, or for serving the best interest of KSA; or
- for other purposes that may be determined by the implementing regulations,

and provided in each case, amongst other things, that the transfer does not prejudice the national interests of KSA and has been approved by the data regulator.

In the absence of the implementing regulations providing further clarity, establishing a legitimate basis for transfers of personal data from KSA is extremely problematic.

National Data Regulations

The National Data Regulations requires that prior written consent of the relevant regulatory authority is sought before transferring personal data out of KSA.

Telecommunication

The Telecom Data Protection Principles requires that service providers process customers' personal data within KSA, and prohibits them from processing customers' personal data out of KSA.

Internet of Things

All servers, devices and network components used in providing an IoT service and all data relating to the service must be located within the Kingdom.

Cloud Services

The Cloud Framework also prohibits transfer of government related data out of KSA.

Financial

The Saudi Central Bank prohibits the transfer of customers' data out of KSA.

10. Data Protection Officer

PDPL

No requirement to appoint a data protection officer but this may be contained in the implementing regulations of the law which are yet to be published.

National Data Regulations

The National Data Regulations requires that a data controller shall establish an organisation unit to be entrusted with personal data protection matters.

Telecommunication

The Telecom Data Processing Principles require that service providers assign the role and responsibilities of customers' personal data protection to an independent function.

11. Security

PDPL

Article 19 of the PDPL requires controllers to take the necessary organizational, administrative and

technical measures and means to ensure the preservation of personal data, including when it is transferred, in accordance with the provisions and controls specified in the implementing regulations which are yet to be published.

National Data Regulations

The National Data Regulations require the use of appropriate security measures.

National Cybersecurity Authority's (the **"NCA"**) has also issued mandatory controls (documents) that address security measures in the context of cybersecurity.

Financial

The Saudi Central Bank's Cybersecurity Framework of 2017 sets out the security measures that need to be taken in the context of cybersecurity.

12. Breach notification

PDPL

The Authority must be notified of data breaches. Unlike GDPR, this must be done immediately and there is no qualitative threshold in relation to the seriousness of the breach. The implementing regulations will define in what circumstances data subjects will need to be notified of the breach.

National Data Regulations

The National Data Regulations requires notification of the relevant regulatory authority and NDMO in the event of a severe data breach.

Telecommunication

The Telecom Data Processing Principles requires that service providers notify CITC immediately when a breach of customers' personal data occurs.

Ecommerce

The Implementing Regulations of the Ecommerce Law require notifying the Ministry of Commerce in the event of a breach of customers' personal data.

Financial

The Saudi Central Bank should be notified in the event of a data breach.

13. Direct marketing

PDPL

Controller's require consent to send or e-mail promotional or awareness materials. There is no "customer exception rule" under the PDPL akin to the e-Privacy Directive framework in Europe.

We note the E-Commerce Law also appears to require express consent to be obtained by E-Commerce Store operators in order to carry out direct marketing to their customers.

14. Cookies and adtech

There is no specific legislation in relation to cookies in KSA.

15. Risk scale

High (heavy)

16. Useful links

- Communication & Information Technology Commission ("**CITC**"): www.citc.gov.sa
- Ministry of Commerce: www.mc.gov.sa
- Saudi Public Prosecution: www.pp.gov.sa
- Saudi Authority for Data and Artificial Intelligence: www.sdaia.gov.sa
- National Data Management Office: www.sdaia.gov.sa/ndmo/

Cybersecurity

1. Local cybersecurity laws and scope

PDPL

Royal Decree M/19 of 9/2/1443H (16 September 2021) approving Resolution No. 98 dated 7/2/1443H (14 September 2021) The Personal Data Protection Law ("**PDPL**") is the main data protection law in KSA. **PDPL takes effect on 23 March 2022 and there is a compliance grace-period of one year until 23 March 2023**. Further implementing regulations are due to be published in advance of the effective date. The PDPL requires controllers to adopt appropriate security measures for personal data akin to the risk-based obligation contained in the GDPR.

Cybersecurity

The Anti-cybercrimes Law of 2007 (the "**Cybersecurity Law**") is a general law that addresses cybersecurity.

The National Cybersecurity Authority (the **"NCA"**) issued certain guidelines and mandatory documents to regulate cybersecurity. These mandatory documents include (i) Essential Cybersecurity Controls of 2018 (the "**ECC**"); (ii) Cloud Cybersecurity Controls of 2020; (iii) Critical Systems Cybersecurity Controls of 2019; and (iv) Remote Work Cybersecurity Controls (English version not available).

There are also other sector-specific laws and other mandatory documents that address cybersecurity.

Telecommunication

The CITC issued the Cybersecurity Regulatory Framework in June 2020 to address cybersecurity risks in the information and communications technology and the postal sector.

Ecommerce

The NCA issued the Cybersecurity Guidelines for ECommerce Service Providers of 2019 ("**CGESP**") and the Cybersecurity Guidelines for ECommerce Consumers of 2019 ("**CGEC**") to address cybersecurity in ecommerce activities.

Financial

The Saudi Central Bank (formerly the Saudi Arabian Monetary Authority) issued theCybersecurity Framework of 2017 (the "**Cybersecurity Framework**") to regulate cybersecurity in the financial institutions regulated by the Saudi Central Bank. These financial institutions include banks, insurance and reinsurance companies, financing companies, and credit bureaus.

2. Anticipated changes to local laws

There are no anticipated changes however implementing regulations to the PDPL are expected to be published

3. Application

PDPL
Article 19 of the PDPL applies to all controllers of personal data and requires them to take the necessary organizational, administrative and technical measures and means to ensure the preservation of personal data, including when it is transferred, in accordance with the provisions and controls specified in the implementing regulations which are yet to be published.

Cybersecurity

While the Cybersecurity Law applies across the board and penalises cybercrimes, NCA's mandatory documents referred to above apply to government organisations in the KSA, including ministries, authorities, and establishments, and government-owned companies and entities, as well as private sector organisations owning, operating, or hosting Critical National Infrastructures ("**NCI**"). The NCA further defines CNIs as assets, such as facilities, systems, networks, processes, and key operators that operate and process them, whose loss or vulnerability to security breaches may lead to certain significant impacts. Further, the applicability will also depend on the technology being used by, or the business of, the concerned organisations.

Telecommunication

The Cybersecurity Regulatory Framework of the CITC applies to service providers in the information and communications technology and the postal sector.

Ecommerce

CGESP and CGEC are both non-binding documents setting out best practices for the protection of ecommerce data and systems. Whilst these are specifically ecommerce related, the banking and transactional aspects of cybersecurity are regulated differently.

Financial

The Saudi Central Bank's Cybersecurity Framework regulates cybersecurity in the financial institutions regulated by the Saudi Central Bank. Said financial institutions include banks, insurance and reinsurance companies, financing companies, and credit bureaus.

4. Authority

- National Cybersecurity Authority: www.nca.gov.sa
- Saudi Public Prosecution: www.pp.gov.sa
- Communication and Information Technology Commission: www.citc.gov.sa
- Saudi Central Bank: www.sama.gov.sa

5. Key obligations

PDPL
Controllers are under a general obligation to protect personal data.

Cybersecurity

The ECC requires notifying NCA of any cybersecurity incidents, as well as sharing incidents notifications, threat intelligence, breach indicators and reports with NCA.

Telecommunication

The Cybersecurity Regulatory Framework of the CITC requires all service providers licensed by CITC that are classified as CNIs to comply with NCA's ECC and is required to report to the CITC in addition to

the NCA.

Financial

A financial institution regulated by the Saudi Central Bank should notify it when a medium or high-classified security incident occurs, and should submit a formal incident report after the incident.

6. Sanctions & non-compliance

Administrative sanctions:

The Cybersecurity Law imposes fines of up to SAR 5m (USD 1.33m) for cybercrimes.

There are fines of up to three million Saudi Riyals (SAR 3,000,000) (approximately USD 800,000) for disclosure or publication of sensitive data in breach of PDPL. The PDPL also introduces a general fine of five million Saudi Riyals (SAR 3,000,000) (approximately USD 1,332,697) for any violation of the PDPL.

Criminal sanctions:

The Cybersecurity Law provides for imprisonment of up to ten years for cybersecurity crimes, depending on the severity of the cybercrime.

Others:

Any equipment used in committing a cybercrime can also be confiscated.

7. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?

Saudi CERT is the national computer emergency response team, which falls under the NCA.

8. National cybersecurity incident management structure

The NCA is the main national authority for managing cybersecurity incidents. However, other regulators such as the CITC and the Saudi Central Bank have their own mechanism for receiving cybersecurity incident reports.

9. Other cybersecurity initiatives

The Saudi Federation for Cyber Security and Programming (SAFCSP) is a national institution under the umbrella of the Saudi Arabian Olympic Committee, which seeks to build national and professional capabilities in the fields of cybersecurity and programming.

10. Useful links

- Saudi CERT: https://cert.gov.sa/en/
- Reporting a vulnerability to Saudi CERT: https://cert.gov.sa/en/report-vulnerability/
- Reporting a cybersecurity incident to NCA: https://nca.gov.sa/en/pages/report_incident.html
- Reporting a cybersecurity incident to CITC: https://www.citc.gov.sa/en/services/Pages/ReportSecurityIncident.aspx
- Saudi Federation for Cybersecurity, Programming and Drones: https://safcsp.org.sa/

Key Contacts

Ben Gibson
Dubai
Partner

Authors

Ben Gibson
Dubai
Partner

Kate Corcoran
Dubai
Senior Associate