Legal 500
Country Comparative Guides 2024

Saudi Arabia

Data Protection & Cybersecurity

Contributor

DROUA AL-AMAL

Saifullah Khan

Director | saifullah.khan@drouaalamal.sa

Saeed Hasan Khan

Director | saeed.hasan@drouaalamal.sa

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Saudi Arabia.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Saudi Arabia: Data Protection & Cybersecurity

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered by them; what sectors, activities or data do they regulate; and who enforces the relevant laws).

The personal data protection law of KSA (PDPL) has been issued pursuant to Royal Decree No. (M/19) dated 09/02/1443 AH corresponding to September 16, 2021 and has been amended pursuant to Royal Decree No.(M/148) dated 05/09/1444 AH corresponding to March 27, 2023.

The PDPL has been enforced on September 14, 2023, with a grace period of one year will be implemented from September 14, 2024. The Saudi Data & Artificial Intelligence Authority (SDAIA) is competent authority to implement and enforce the PDPL.

The Implementing Regulation of the PDPL and the Regulation on Personal Data Transfer outside the Kingdom have also been issued.

The Anti-Cyber Crime Law 2007 issued by Royal Decree No. M/17 0n 8 Rabi'I 1428H (March 26, 2007), criminalizes invasion of privacy and illegal and authorized use, access and modification of data which includes but not limited to the spying or illegal interception or reception of data transmitted through an information network or a computer, also it criminalizes the unlawful access to the computers with the motive of blackmailing or threatening any person.

The kingdom has also established a national cyber security authority established by Royal Decree No. 6801 of October 31, 2017, as amended by Royal Decree No. 7053 of September 9, 2021.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2024–2025 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments (together, "data protection laws"))?

SDAIA has issued, for public consultation, draft amendments to the Regulations on Personal Data Transfer outside the Kingdom. It is expected that new/amended regulations on cross-border of transfer of personal data will soon be issued.

3. Are there any registration or licensing requirements for entities covered by these data protection laws, and if so what are the requirements? Are there any exemptions?

Article 34 of the Implementing Regulations of the PDPL provides that SDAIA (the competent authority) is to issue rules for registration, of controllers, in national register. The rules have not yet been issued.

4. How do these data protection laws define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data") versus special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction?

Personal Data:

Any data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual, including name, personal identification number, addresses, contact numbers, license numbers, records, personal assets, bank and credit card numbers, photos and videos of an individual, and any other data of personal nature.

Sensitive Data:

Personal Data revealing racial or ethnic origin, or religious, intellectual or political belief, data relating to security criminal convictions and offenses, biometric or Genetic Data for the purpose of identifying the person, Health.

Data Subject:

The individual to whom the Personal Data relate.

Controller:

Any Public Entity, natural person or private legal person that specifies the purpose and manner of Processing Personal Data, whether the data is processed by that Controller or by the Processor.

Processor:

Any Public Entity, natural person or private legal person that processes Personal Data for the benefit and on behalf of the Controller.

Processing:

Any operation carried out on Personal Data by any means, whether manual or automated, including collecting, recording, saving, indexing, organizing, formatting, storing, modifying, updating, consolidating, retrieving, using, disclosing, transmitting, publishing, sharing, linking, blocking, erasing and destroying data.

Collection:

The collection of Personal Data by Controller in accordance with the provisions of this Law, either from the Data Subject directly, a representative of the Data Subject, any legal guardian over the Data Subject or any other party.

Personal Data Breach:

Any incident that leads to the Disclosure, Destruction, or unauthorized access to Personal Data, whether intentional or accidental, and by any means, whether automated or manual.

Explicit Consent:

Direct and explicit consent given by the Data Subject in any form that clearly indicates the Data Subject's acceptance of the Processing of their Personal Data in a manner that cannot be interpreted otherwise, and whose obtention can be proven.

Health Data:

Any Personal Data related to an individual's health condition, whether their physical, mental or psychological conditions, or related to Health Services received by that individual.

5. What are the principles related to the general processing of personal data in your jurisdiction?

For example, must a covered entity establish a legal basis for processing personal data, or must personal data only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

The Controller/processor shall process personal data while considering the following principles:

- The consent of the data subject is mandatory except in cases where exception has been given.
- The purpose for which personal data is to be collected shall be directly related to the Controller's purposes.
- The purpose for personal data is collected must not be in contravention with any legal provision.
- The means and methods used for the processing of personal data must be clear, secure and shall not involve any deception, misleading or extortion.
- The means and methods used for the processing of personal data must not be against any existing legal provisions.
- The personal data collected must be appropriate, that is it must be minimum and up to the extent it is needed for the purpose for which it was collected.
- The personal data collected must not be retained any longer than it was needed.
- The controller may not process the personal data without taking the sufficient steps to verify the Personal Data accuracy, completeness , timeliness and relevance to the purpose for which it was collected.

6. Are there any circumstances for which consent is required or typically obtained in connection with the general processing of personal data?

Consent of data subject is mandatory for every processing of the personal data except in cases when the exemption has been provided in the law. Furthermore the controller/processor has to obtain the consent if the purpose for the processing has to be changed.

The Data subject's consent has to be explicit in the following cases;

- When the processing involves sensitive data
- When the processing of credit data is carried out.

- When the decisions are made solely based on automated processing of Personal Data.

Following are the circumstances when the controller/processor are permitted to process personal data without obtaining of the consent;

- When the processing of the personal data is in the interest of the data subject but it is impossible or difficult to contact /reach out the data subject.
- When the processing is mandatory with respect to another law.
- When the processing is necessary for the execution of an agreement to which data subject is already a party.
- When the controller is a public entity and the processing of the personal data of the data subjects is necessary for the;
    i. Security purposes
    ii. For the judicial purposes.
- When the processing is necessary to be done by the Controller for its legitimate interest, the controller can process personal data without any consent of the data subject if it does not prejudice the rights and interests of the Data subjects. It is also important that such processing must not involve the sensitive personal data.

7. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

The Controller shall obtain the consent for the processing of the personal data as follows:

- In appropriate form or means
- consent can be written or verbal or can be obtained by use of any electronic methods.

While obtaining of the consent through appropriate form and means the following conditions are to be met:

i. The consent obtained must be given freely by the data subject and consent shall not be obtained through misleading methods.
ii. The data subject must be intimated about the purpose for which data is to be processed, the purpose must be disclosed to the data subject at the time of obtaining of consent of beforehand. The purpose for which personal data is to be processed must be clear and specific.
iii. The data subject giving the consent must have a legal capacity to give the consent.
iv. The consent obtained must be documented for future verification purposes , the documentation may be done by:
    - Keeping the records that must include the consent of the data subjects with respect to the processing
    - The records must contain the consent along with the time when consent was taken and also the method through which consent was obtained.
v. For each processing operation independent consent must be obtained.

8. What special requirements, if any, are required for processing sensitive personal data? Are any categories of personal data prohibited from collection or disclosure?

In respect of sensitive personal data, the PDPL provides:

- No sensitive personal data can be processed without the obtaining of data subject's consent.
- Even when the controller can receive personal data from another source than the data subject for the any legitimate purpose, the controller is barred from obtaining sensitive personal data from any other source than the data subject.
- No sensitive data can be processed for the marketing purposes..
- Processing for the purposes of scientific, research or statistical purposes is allowed without consent, however processing is not allowed without consent for these purposes in case of sensitive personal data.

9. How do the data protection laws in your jurisdiction address health data?

The law has defined the health data as mentioned in Question No.4.

The Controller is under obligation to adopt such mechanism which will safeguard the processing of the Health data. The controller has to adopt the following

standards/measures:

- While processing the personal health data of an individual a controller shall take such technical, administrative and organizational measures that will safeguard the personal health data from any unauthorized use, misuse, its use for any other purposes than for which it was processed and breach of health data.
- The controller has to adopt such procedures that will guarantee the preservation of the personal health data, for this reason the controller has to adopt and implement the requirements and controls issued by the:
    - Ministry of Health
    - The Saudi Health Council
    - The Saudi Central Bank
    - The Council of Health Insurance
    - Any other organizations involved in regulation of health services and health insurance services i.e. those that specify the tasks and responsibilities of employees of health care providers, health insurance companies, health insurance claims management companies and also of those entities which are contracted by these organizations to carry out the processing of health data.
- The Controller of the Health data must make the internal policies with respect to data privacy laws and regulations.
- While collecting of the personal data the responsibilities must be distributed among the employees in such possible manner which prevent overlapping specialization along with that employee's access to personal data must be managed in such a manner that it would guarantee the highest degree of the privacy of the data subjects.
- All stages of the health data processing must be documented. The data subjects must be provided with such means which would help identify the in charge of each stage of health data processing.
- Where a Controller has to hire a processor for the processing of the personal data, the controller while concluding an agreement with the processor must include in it the obligations which are being conferred by the law on the Controller.
- The health data processing must be carried out at minimum and only when it is necessary to provide the health care services and products of health insurance programs.

10. Do the data protection laws in your jurisdiction include any derogations, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

The PDPL excludes the individual's personal data processing from its scope when the processing is carried out for family and personal use and does not go beyond it.

11. Do the data protection laws in your jurisdiction address children's and teenagers' personal data? If so, please describe how.

The PDPL enables the legal guardian to act on behalf of a data subject who is lacking his/her legal capacity fully or partially. The legal guardian has to act in the best interest of the data subject.

A legal guardian on behalf of the data subject can exercise his/her (data subject's) rights given by the PDPL. Moreover, a legal guardian can also give consent on behalf of the data subject.

While taking consent of the data subject who lacks fully or partial legal capacity through its legal guardian the validity of the guardianship over the data subject must be verified by the controller.

12. Do the data protection laws in your jurisdiction address online safety? Are there any additional legislative regimes that address online safety not captured above? If so, please describe.

The Anti-Cyber Crimes Law of 2017 governs the cybercrimes in the Kingdom. The Saudi Arabian Monetary Authority (SAMA) has established a Cyber Security Framework which issues standards and guidelines to promote Cyber Security activities for the financial sectors.

The Anti-Cyber Law has categorized different online offences and has set penalties as under:

a) If an individual is involved in the commission of the following crimes, he will be punished with a term not exceeding one year and or a fine not exceeding 500,000:

- To illegally access a computer with an intention to black mail or threaten a natural or legal person or to force him/her to do anything or restrict him/her from doing any thing.
- If defamation campaign is done by the use of any of the information technology devices.
- The privacy of a natural person is breached by taking a photo or making of a video.

b) A person involved in the commission of the following crimes shall be punished with an imprisonment not exceeding 3 years and a fine not exceeding 2,000,000 Riyals, or either penalty:

- Illegal access to bank or credit data or data pertaining to the ownership of securities and illegal access to such data for obtaining of the data, information, funds, services offered.
- Acquisition of moveable property of bonds,

c) Whoever shall commit the following crimes with respect to the online material available shall be punished with imprisonment for a time period not exceeding 4 years and a fine not exceeding 3,000,000 Riyals or either penalty:

- Hacking of the online database, and distortion, deletion, destruction , damage and altering of the private data.
- Causing obstruction for the information network.
- Obstruction of services by any means.

d) Anyone who will commit the following crime shall be punished with an imprisonment not exceeding 5 years and a fine up to 3,000,000 Riyals or either penalty:

- Transmission, preparation, production or storage of material that is inconsistent with the public order, religious values, morality or which breaches the privacy of the natural person.
- Development of any website to promote human trafficking.
- Publication of pornographic material.
- The development of a website on information network or computer to trade, distribute, demonstrate methods of use, or facilitate dealing in narcotics and psychotropic drugs.

13. Is there any regulator in your jurisdiction with oversight of children's and teenagers' personal data, or online safety in general? If so, please describe, including any enforcement powers. If this regulator is not the data protection regulator, how do those two regulatory bodies work together?

Overall SDAIA is entrusted to oversight personal data of all data subjects including children's and teenager's personal data.

14. Are there any expected changes to the online safety landscape in your jurisdiction in 2024–2025?

No public information is available in this regard.

15. Does your jurisdiction impose 'data protection by design' or 'data protection by default' requirements or similar? If so, please describe the requirement(s) and how businesses typically meet such requirement(s).

The PDPL has not any such provision regarding "data protection by design" or "data protection by default".

16. Are controllers and/or processors of personal data required to maintain any internal records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

The controller is required to maintain the record of the processing activities during the period of the processing and also for 5 years after the completion of the personal data processing activity. The term of 5 year shall start from the date of completion of the personal data processing activity.

Record of processing activities must include the following ingredients:

a. Name & contact details of the controller
b. Where applicable, the information of the data protection officer
c. Purpose for which personal data is being processed or to be processed.
d. Details of Categories of personal data being processed and the categories of data subject.
e. Where possible retention period of each category of personal data
f. Categories of the recipients with whom the

personal data is to be shared
g. Descriptions of personal data which is to be transferred out side of the Kingdom

17. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? If so, please describe such requirement(s).

The PDPL stipulates the circumstances when a controller is allowed to retain the personal data processed by it or when it has to be deleted.

The Controller has to delete the personal data without undue delay once it is no longer needed for the purpose it was collected, or the purpose for which it was collected cease to exist. After the deletion it must be made sure the destroyed data must not anything which may lead to the identification of the data subject.

There are circumstances when the personal data can be retained even after the purpose for which it was collected cease to exist. Such circumstances are as follows:

- When the law has provided legal basis for retaining of the personal data for specific period even after the purpose for which personal data was processed ceased to exist. The controller shall destroy the personal data once the specific time period lapses or when the purpose of the collection is satisfied, whichever is higher.
- When the personal data collected is relevant to any judicial proceedings before any judicial authority and its retention is required for the purpose of judicial proceedings in that case personal data shall be retained and will be destroyed once the judicial proceedings are being concluded.

Personal Data Disposal:

The Controller shall dispose the personal data when:

- The personal data is no longer required.
- When the data subject requests of such destruction of personal data.
- The data subject withdraws its consent and the consent was the sole legal basis for the processing.
    - The Controller came to know that their personal data processing is in violation of law.

While disposing of personal data being processed, following conditions are to be met by the Controllers:

- The controller shall adopt appropriate measures to notify any other parties of such destruction of personal data, with whom the controller has shared the personal data and shall request of destruction of personal data.
- The controller has to take appropriate measures to notify the individuals with whom he has shared the personal data about the decision to destroy personal data and shall request them to destroy personal data in their possession as well.
- The Controller shall destroy all copies of personal data he had with it including any backups in the system, and any other copy in its system.

18. Under what circumstances is a controller operating in your jurisdiction required or recommended to consult with the applicable data protection regulator(s)?

There is no such requirement in the PDPL.

19. Do the data protection laws in your jurisdiction require or recommend risk assessments in connection with data processing activities and, if so, under what circumstances? How are these risk assessments typically carried out?

The Controller has to formulate risk assessment in a written and documented form. The assessment shall underline the potential impacts and risks that may have affect the data subject of personal data processing. The Controller shall provide a copy of impact assessment to any processor acting on its behalf in relation to the relevant processing.

If the assessment shows that processing operations will harm the privacy of data subjects then the Controller shall address the reasons for that and re-conduct the assessment.

Impact assessment is to be conducted in the following cases:

- When sensitive personal data is being processed
- When the personal data collected from two different sources are being collected, compared or linked.

- Incase the Controller on continuous and large scale, process personal data of data subjects who fully or partially lack legal capacity or when processing is of such nature that it requires continuous monitoring of data subjects.
- When the controller is using new technologies for the processing of the personal data
- When the controller based its decision solely on automated processing of the personal data.
- When the Controller is providing a product or service that involves processing of the personal data that is likely to cause harm to the privacy of data subjects.

The impact assessment document must comprise of the following:

a. Purpose for which personal data is to be processed and legal basis of the processing.
b. The nature of the processing
c. Types of personal data to be processed
d. Sources of the personal data
e. Entities with whom personal data is to be shared.
f. Scope of the processing (type of personal data and geographical scope of processing)
g. Context of the processing which identifies the relationship between the data subjects, controller and the processors.
h. Necessity and proportionality of the measures which are to be taken to enable the Controller and Processors to process the minimal Personal Data necessary to achieve the purpose of processing.
i. Impact of processing such as likelihood of any negative impact on data subjects
j. Proposed measures that needed to be adopted to prevent or limit the risks.

20. Do the data protection laws in your jurisdiction require a controller's appointment of a data protection officer, chief information security officer, or other person responsible for data protection, and what are their legal responsibilities?

The Controller need to appoint a data protection officer if it is a public entity that provide services and involves large scale of personal data processing. If a controller is involved in such activities primarily which involves the processing operations requiring continuous and regular monitoring of individuals on large scale then such data controller shall also in need of data protection officer appointment.

The Controller shall also appoint a data protection officer if it is involved in processing of the sensitive personal data.

The data protection officer may be an official, an employee or an external contractor of the controller.

Responsibilities of data protection officer:

- Monitoring the implementation of the provisions of the law and regulations
- Monitoring the procedures adopted by the controller
- Receiving and handling the requests pf the data subjects with respect to the personal data
- Acting as the direct point of contact between the controller and the competent authority and implementing its decisions and regulations.
- Supervising the impact assessment, audit reports, evaluation with respect to data protection controls, documenting the assessment results and issuing necessary recommendation accordingly
- Facilitating data subjects in the exercise of their rights.
- Notifying the competent authority with respect to the breach incidents.
- Handling and responding to data subject's requests
- Overseeing the records of personal data processing activities of the Controller
- managing the Controller's violations and acting accordingly to correct the wrongdoings.

21. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s).

No such specific requirement is there in the PDPL. However, the PDPL do require to implement organizational and administrative measures to protect the personal data. This implies the employee training as part of the organizational measures.

22. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s)

(e.g., posting an online privacy notice).

The PDPL stipulates that appropriate measures shall be taken to inform the data subjects with the information prior to the processing of their personal data. There are two situations when the data is to be collected one directly from that data subject and from any other individual other than the data subject.

The following information is be intimated to data subjects prior to the processing:

- Legal basis for processing
- The purpose of collection and controller shall specify the personal data whose collection is mandatory and whose collection is optional.
- Unless the collection of the personal data for security purposes, the identity of the person collecting the personal data and the address of its representative, if necessary.
- The entities with which personal data will be shared.
- The potential consequences and risks that may result from not collecting the personal data.

When the personal data is directly processed from the data subject, following information is to be provided to data subjects:

- Controller's identity, its contact details, details of any other channel/means of communication with data subjects for personal data protection processing.
- Where applicable, contact details of the data protection officer.
- Legal basis for processing.
- Specific, clear and explicit purpose for collecting and processing personal data.
- The time period for which personal data is to be retained and if that is not possible the estimated time period for which personal data may be retained.
- Information with respect to rights of data subjects.
- Information with respect to withdraw of the consent by the data subject.
- Whether processing of personal data is mandatory or optional.

When the personal data is to be collected directly from the individual other than the data subject, the controller is under obligation to communicate to data subject of above mentioned information within 30 days. Along with the above mentioned information, the data subject shall also be communicated o categories of persona data processed and the source from which it is obtained.

The PDPL also gives some exceptions when aforementioned information needs not to be given to data subject:

- The information is already available to the data subject.
- The implementation of this (to inform data subject) is not possible or requires disproportionate effort.
- The data is being obtained in accordance with law.
- The controller is a public entity and collection of personal data is for security purpose, judicial requirements or to achieve public interest.
- Personal data is subject to professional confidentiality provisions established by law.

Also in case of additional processing of personal data for a purpose other than for which it was collected , the controller need to provide the additional necessary information.

23. Do the data protection laws in your jurisdiction draw any distinction between the controllers and the processors of personal data, and, if so, what are they?

As per answer to question 4.

24. Do the data protection laws in your jurisdiction place obligations on processors by operation of law? Do the data protection laws in your jurisdiction require minimum contract terms with processors of personal data?

The law confers this obligation upon the Controller to take sufficient guarantee from the processor to protect the personal data while processing personal data. The terms of agreement can be defined with mutual understating and no such time limit has been defined by the law.

The Agreement between the Controller and the processor must comprised of the following ingredients:

- Purpose of processing
- Categories of the personal data being processed.
- Duration of the processing

- Processor's commitment to notify the Controller without undue delay, in case of a personal data breach, in accordance with the provisions of the Law, this Regulation.
- The processor has to be clarified of the fact that whether the processor is subject to regulations in other countries and the impact on their compliance with the law and its regulations.
- Not requiring the data subject's prior consent for mandatory disclosure of personal data under the applicable laws in the kingdom, provided that the processor notifies the controller of such disclosure.
- Identifying any subcontractors contracted by the processor, or any other party to whom personal data will be disclosed.

25. Are there any other restrictions relating to the appointment of processors (e.g., due diligence, privacy and security assessments)?

No such restrictions with respect to the appointment of the processors has been imposed.

26. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these terms defined, and what restrictions on their use are imposed, if any?

The National Data Management Office (NDMO) has issued, as part of National Data Governance Policies, Children and Incompetents' Data Protection Policy (the Policy) which provides that controllers should not make automated decisions based on a child's or incapacitated person's Personal Data Processing and must not use it for direct marketing.

27. Please describe any restrictions on targeted advertising and/or cross-contextual behavioral advertising. How are these terms or any similar terms defined?

Without prejudice to any other law in the land the controller may not use personal means of communication which includes the postal address, email address of the data subject to send advertising or awareness-raising materials, however public entities can send awareness-raising material.

While for the purpose of sending awareness-raising material and advertising the control has to follow the following steps;

- Has to obtain the consent from data subject
- The controller must provide a mechanism that would allow the data subject to opt out of receiving marketing materials. Such mechanism must be easy, straightforward, and at least as easy as the procedures for giving consent to receive them.
- While sending the marketing materials, the identification of the entity sending the marketing material shall be clearly stated without any anonymization.
- Where a data subject shall withdraw its consent, the controller shall immediately cease the process of sending related marketing materials without undue delay.

28. Please describe any data protection laws in your jurisdiction addressing the sale of personal data. How is the term "sale" or such related terms defined, and what restrictions are imposed, if any?

The PDPL doesn't address the sale of the personal data.

29. Please describe any data protection laws in your jurisdiction addressing telephone calls, text messaging, email communication, or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

Telecommunication and Information Technology Act (the Act) governs the telecommunication sector within the Kingdom .

It has defined telecommunications as "any transmission or reception, between persons or things, of signs, written messages, images, sounds, or information of any kind via wired or wireless systems."

The Act is promulgated to create such environment in the kingdom which is feasible for technical innovation, entrepreneurship, research and development in Telecommunication & IT Sector. The law aimed at to support the innovation and development of developing sub sectors and new technologies and also to encourage new telecommunications and information technology services.

While providing a support to emerging IT,

telecommunication and entrepreneur sector the law also safeguard the public interest by providing protection to the end users of the above mentioned sectors by providing appropriate quality if IT and Telecommunication services. Furthermore, the telecommunication Act is also in field to provide protection to the user of services against harmful content, and strive to maintain the confidentiality of communications.

The Bye Laws of the Act have further given protection to the confidentiality of user's communication and also protected personal information of the users. For protection of the user's information the law is in line with the personal data protection law in terms of being specific, clear purpose for which it is collected, must be accurate and up to date and that user's information and communications are protected by means and methods proportionate to their sensitivity.

Some of the important definitions from the Telecommunication bye laws are as follows:

Mobile Telephony Service:

Wireless communication service that enables telecommunications between portable wireless devices, including:

a. Fixed telephone devices.
b. Fixed wireless devices.
c. Space stations.
d. Other portable wireless devices.

Person:

A natural or legal person, including any governmental authority or shareholding company, or a limited or joint liability company, or other types of companies and individual establishments.

30. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined, and what restrictions are imposed, if any?

The biometric is included with in the definition of sensitive personal data.

31. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

The SDAIA has issued its Al Ethic Principles (Version 1.0) in September, 2023, to regulate the activities related to the AI in the Kingdom, also the Saudi Authority for Intellectual Property (SAIP) has also issued amendments in its previous intellectual property legislation, which would also regulate the intellectual property rights to be created for the AI creation.

32. Is the transfer of personal data outside your jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

The PDPL and the Regulation on Personal Data Transfer outside the Kingdom provides for the procedure and manner in which the personal data may be transferred outside the Kingdom.

- A Controller is allowed to transfer or disclose personal data outside the jurisdiction if it transfers it in accordance with the law and regulations. While transferring the controller must ensure that such transfer doesn't impact national security or vital interests of the kingdom or violate any other laws of the kingdom.
- the Controller shall have to minimize and limit the data transfer to the outside the jurisdiction to the extent it will serve the purpose for which personal data is to be transferred.
- There is an adequate level of protection for personal data outside the kingdom which must be at least equivalent to the level of protection guaranteed by the law.
- When transferring or disclosing personal data outside the kingdom the Controller must ensure that the privacy of the data subjects is not harmed and also that it doesn't not impact the level of the protection guaranteed for personal data under the law and its regulations. For this purpose, the controller has to ensure that the transfer or disclosure of the personal data doesn't compromise the following:

    a. The data subject's ability to exercise their rights
    b. The data subject's ability to withdraw their consent for the processing.

c. Controller's ability to comply with the requirements of notifying the personal data breach.
d. Controller's ability to comply with provisions, controls, and procedures for disclosing of the personal data.
e. Controller's ability to comply with the provisions and controls for destroying personal data.
f. Controller's ability to take necessary organizational and technical measures.

The competent authority shall evaluate the level of protection of the personal data provided in the recipient jurisdiction. The competent authority shall submit the results of the assessment (including its recommendations) of the level of protection for Personal Data outside the kingdom and shall also give its recommendation to whether an adequacy decision must be issued or not or an international agreement must be concluded. The competent authority shall review the assessment after every 4 years if it is necessary. The competent authority shall propose to the Prime Minister the termination, amendment, or suspension of any decision taken regarding the level of protection outside the kingdom.

Where no adequate level of protection is available outside the kingdom where personal data has to be transferred, it must be ensured that the regulatory requirements in the country or the international organization do not bring any prejudice to the privacy of the data subject or hinders the enforcement of the appropriate safeguards.

The appropriate safeguards may constitute any of the following:

- Binding Common Rules
- Standard Contractual Clauses
- Certificate of compliance with the PDPL and its regulations in the kingdom, together with the enforceable commitments of applicability of the appropriate safeguards, must be given by the Controller or Processor in the third country.
- Binding Codes of Conduct.

EXEMPTIONS:

In the absence of adequate level of protection for the personal data and in absence of any of the appropriate safeguards, the transfer of personal data outside the Kingdom or disclosure to a party outside the Kingdom is permitted in any of the following circumstances;

1. When the transfer of personal data outside the kingdom is necessary for the performance of an Agreement.
2. When the controller is a public entity and the transfer of personal data outside the kingdom is necessary for the safeguards of the kingdom's national security or for the public interest.
3. When the controller is a public entity and the transfer of personal data outside the kingdom is necessary for the investigation or detection of crimes, or such transfer is necessary for the prosecution of perpetrators, or when the transfer is necessary for the execution of penal sanctions.
4. When the transfer of personal data outside the kingdom is necessary for the protection of vital interests of the data subjects.

33. What security obligations are imposed on data controllers and processors, if any, in your jurisdiction?

The PDPL requires the Controller to take the necessary organizational, administrative , and technical measures to ensure the security of the personal data and the privacy of the data subjects.

The Controller has to implement necessary technical and security measures to limit the security risks related to Personal Data Breach.

The Controller has to comply with the relevant controls, standards issued by the National Cyber Security Authority or other recognized best practices of cyber security if the Controller does not fall within the domain of National Cyber Security Authority.

The Controller while hiring a processor has to conclude an agreement with the processor wherein the Controller has to take guarantee from the processor that it would take appropriate measures to protect the security of the personal data.

34. Do the data protection laws in your jurisdiction address security breaches and, if so, how do such laws define a “security breach"?

Personal data breach has been defined as “any incident that leads to the Disclosure, Destruction, or un authorized access to Personal Data, whether intentional or accidental, any by any means, whether automated or manual."

Notification to the Authority (SDAIA):

The Controller upon becoming aware of any data breach incident that would potentially cause harm to the personal data or data subject's rights , shall notify the SDAIAA of any such breach incident within 72 hours of the breach. Where the Controller will fail to notify the SDAIAA within the stipulated time period it shall act on it as soon as possible and will also justify the delay in the intimation of the data breach incidents.

The notification to the authority (SDAIA) must include the following information:

a. Complete detail of the incident of personal data breach , including the time, date and circumstances of the breach and the time when the Controller became aware of the breach.
b. Categories of effected personal data
c. Approximate number of data subjects who got effected of the breach.
d. The types of personal data which became target of breach incident.
e. Description of the actual or potential risks impact of such breach incident on personal data and data subjects.
f. Details of the measures taken by the Controller to prevent or limit and mitigate the impact of the actual or potential risks to be faced personal data or data subjects along with the details of any future measures that will be taken to avoid the recurrence of the breach.
g. A statement underlining the fact that the data subject has been intimated of his/her personal data breach.
h. The contact details of the Controller or data protection office or any other relevant official who is having information with regard to the data breach.

The controller shall keep the record of the report submitted to the authority with respect to the incident of data breach and shall document the corrective measures it has taken in this regard.

Notification to the data subject:

If an incident of personal data breach may cause damage to the personal data of the data subject or may conflict with their rights or interests, then the Controller is under obligation to notify the data subject of such breach incident without undue delay. The notification furnished must be in a simple and clear language and must constitute the following information:

a. Description of personal data breach
b. Description of potential risks arising from the personal data breach, and the measures taken to prevent or limit those risks and limit their impact.
c. Name and contact details of the controller or data protection officer (if appointed) and any other available means of communication.
d. the controller has to provide data subject with such recommendations or advice that may assist the data subject in taking measures to avoid the identified risk or limit their impact.

35. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecom, infrastructure, AI)?

The telecommunication Act 2022, impose restrictions on the telecommunication service providers while the Saudi Data and Artificial Intelligence Authority (SDAIA) has issues AI Ethic Principles for regulating the AI usage.

The Saudi Arabian Monetary Authority (SAMA) has developed Cyber security framework which consist of mandatory guidelines formulated to strengthen cyber security of the financial institutions regulated by the SAMA, against any threats.

36. Under what circumstances must a business report security breaches to regulators, impacted individuals, law enforcement, or other persons or entities? If breach notification is not required by law, is it recommended by the applicable regulator in your jurisdiction, and what is customary in this regard in your jurisdiction?

The Controller/business has to notify the Competent Authority within 72 hours of the incident of personal data breach, if such breach poses potential harm to personal data or data subject.

37. Does your jurisdiction have any specific legal requirements or guidance for dealing with cybercrime, such as in the context of ransom payments following a ransomware attack?

The Anti-Cyber Crime law of 2007 regulates the cybercrimes within the Kingdom.

The purpose of this law is to identify the cybercrimes

committed and to determine their punishments accordingly. the imposition of the punitive punishments , imprisonments or either of the penalty is to make sure that:

- the information security is being enhanced,
- the protection of rights of users pertaining to legitimate use of computers and information network.
- The public interest, common values and moral is being safeguarded.
- The national economy is protected.

In order to give an overall protection to the individuals, financial activities, users of information networks, computers, the Act has defined the punishments to be received by the any person who commits the Cybercrime.

Following acts has been attributed as the cyber- Crimes:

- Spying on, interception or reception of data transmitted through an information network or a computer without a legitimate authorization.
- Any unauthorized action which is taken with the intention to blackmail or threat any person in order to him to perform an act or to refrain him from doing certain act(the act may be legal or illegal).
- Any unauthorized access to a website or hacking a website for the purpose of changing its design, modify or destroy it, or occupy its URL.
- Invasion of the privacy through the camera equipped mobile phones or the like.
- Defamation and infliction of damage upon others through the use of various information technology devices.

The law has identified various other activities relevant to unauthorized access to network, transmission/ production of inappropriate data as cyber crimes and has suggested punishments accordingly, it has also suggested punishments and fines for the mode of commission of these crimes.

38. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

The National Cyber Security Authority (NCA) has been established to look into the matters pertaining to the Cyber Security in the Kingdom. The NCA is established to protect the Cyber Security Infrastructure in the Kingdom and to issue cyber security guides and frameworks.

The Saudi Arabian Monetary Authority (SAMA) has also developed a Cyber security framework to enable the financial institutions regulated by the SAMA, to identify and address the risks associated with the Cyber Security.

39. Do the data protection laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, any exceptions and any other relevant details.

The PDPL confers the following rights on data subjects which are exercisable through a submission/request made by the data subject to the data controller, which has to be implemented on within 30 days of the request while such time period can be extended;

- Right to be informed
- Right of access to personal data
- Right to request Access to personal data
- Right to Request Correction of personal data
- Right to request Destruction of Personal Data

Right to be Informed:

A – If the personal data is collected directly from the data subject, the controller shall have to inform the data subject about the following details, before or at the time of the collection of the personal data;

- Controller's identity, contact details, and any others means of communications established by the Controller for the purpose of communication of data subject with the controller.
- Where data protection officer is appointed, its contact details.
- The legal basis for which personal data is being collected.
- The clear and specific purpose for which personal data is to be collected.
- Retention period of personal data.
- Data subject's rights awareness
- Information with respect to the withdrawal of the consent by the personal data.
- Information with regard to the nature of the processing, whether mandatory or optional.

The condition of informing the data subject with respect to the processing would not be applicable if the data subject is aware of all the information which is usually

intimated to him/her through the information notice, or if the provision of such information of processing will conflict any other existing law in the kingdom.

B- When Data is obtained from any other person than data subject:

When the personal data of a data subject is obtained directly from any other individual than the data subject itself, the controller is under obligation to inform data subject with the set of information as described in part A, within a period of 30 days. In addition to the information stipulated in Part A the data subject shall has to be intimated of the categories of the personal data processed and the source from which the controller obtained it.

However these conditions are not applied in the following circumstances if ;

- The information is already available to the data subject.
- The execution of the process is impossible or requires disproportionate effort.
- That controller obtained the data in accordance with law.
- The controller is a public entity and the collection of the personal data to is to fulfill and judicial requirement, for security purposes or to protect any public interest.
- The personal data is subject to professional confidentiality provisions established by law.

C- CONTINOUS AND LARGE-SCALE PERSONAL DATA PROCESSING of data subject lacking legal capacity;

When a controller is involved in such business which requires continuous and large scale processing of personal data;

- of individuals that lack legal capacity fully or partially; or
- controller monitor data subjects continuously; or
- controller adopt new technologies; or
- controller make automated decisions based on personal data;

The information so provided shall be in an appropriate language as stipulated in this Article when the controller has this knowledge that data subject fully or partially lacks legal capacity.

Then the controller shall take necessary measures to inform the data subject about the details of the information provided as in section A. the controller while communicating such information gas to furnish following additional information to the data subject;

a. means and methods of collecting and processing Sensitive Data, where applicable.
b. Means and procedures taken to protect personal data.
c. Information with respect to any decisions that will be made based solely on automated processing of personal data.

When a controller starts additional processing of personal data for a purpose other than the one for which it was initially collected for, it shall provide the data subject with the necessary information, before the additional processing, as provided in the law and described in Section A herein.

RIGHT OF ACCESS TO PERSONAL DATA:

a data subject can exercise his/her right to access the personal data in the following cases;

- The exercise of right to access by a data subject will not have a negative impact on the rights of others.
- An access to personal data can be provided when a request to access has been made or when the controller has already provided a channel which enable the data subject to directly access their personal data without the need to make a request.

also while enabling data subjects to access their personal data, the controller must ensure that it does not involve disclosing personal data that identifies another individual.

RIGHT TO REQUEST ACCESS TO PERSONAL DATA:

the law has conferred this right to a data subject that he/she can request a copy of their personal data in a readable and clear format, however the following conditions are to be considered while exercising of this right;

- Exercising of this right to request access to personal data by a data subject should not be negatively impact the rights of others.
- The personal data must be provided to the data subject in a commonly used electronic format and the data subject my request a printed hard copy if feasible.
- While granting access to data subject to his/her personal data, the controller has to ensure that it does not involve disclosing

personal data that identifies another individual.

RIGHT TO REQUEST CORRECTION OF PERSONAL DATA:

If a data subject contest the accuracy of the personal data processed by the controller, the data subject shall have the right to restrict the controller from processing of the personal data for such time period during which the controller will verify the accuracy of the personal data. However, such restriction will not be implemented upon if providing of such data contravenes provisions of the PDPL.

The controller may ask the data subject to provide with needed supporting documents or evidence to verify in order to update, correct, or complete the personal data. the controller shall destroy such documents/ evidences once the verification process will be completed.

After correction of the personal data the Controller, without delay, shall notify the other parties of such correction to whom the personal data has been shared previously.

RIGHT TO REQUEST DESTRUCTION OF PERSONAL DATA:

Controller shall destroy personal data in the following cases:

- When such deletion is requested by the data subject.
- When the personal data is no longer necessary for the purpose it was collected;
- When the data subject withdraws its consent and it was the sole legal basis for processing.
- When the Controller became aware of the fact that the personal data was processed in a manner that violates the law.

The data controller shall destroy the personal data in the following manner:

- When a controller shall has to destroy personal data or when the data subject requests the destruction of the personal data , the controller shall take appropriate action to notify other parties with whom the concerned the personal data has been shared by the Controller .
- The controller shall take appropriate measures to notify the individuals to whom the personal data has been disclosed by any means and to request its destruction.
- The controller shall has to destroy all copies of the personal data it has, whether is its control system or backups .

The PDPL has set out certain exceptions where the controller can retain the data after completion of purpose such as when the data subject is not identifiable through such data, or there are legal basis for the retention of the personal data even after the purpose for which it was collected cease to exist.

40. Are individual data privacy rights exercisable through the judicial system, enforced by a regulator, or both?

The individual can file a complaint before the competent authority within 90 days after he/she became aware of the violation of the PDPL. The competent authority shall assess the complaint and shall decide whether to accept a complaint or not.

The PDPL while protecting the rights of the data subjects also afford this opportunity to the individuals that suffered a damage due to the violation of PDPL and its regulations may apply to a competent court for proportionate compensation for the material of moral damage.

41. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

As per answer at question 40.

42. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual damage to have been sustained, or is injury to feelings, emotional distress or similar sufficient for such purposes?

As per answer at question 40.

43. How are data protection laws in your jurisdiction enforced?

As the PDPL has not been practically implemented so there is no information on the enforcement trend.

44. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

Following penalties are provided in connection with the

violations of the PDPL:

Disclosure of publishing of Sensitive Personal Data in violation of PDPL	Imprisonment not exceeding 2 years and/or a fine note exceeding SAR 3,000,000
Any other violation of the PDPL Law	Fine not exceeding SAR 5,000,000

The fine may be doubled if the violation is repeated, however, the fine will not exceed twice the amount of maximum limit of fine.

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

No such guidelines are published with respect to the calculation of the fines.

46. Can controllers operating in your jurisdiction appeal to the courts against orders of the regulators?

The data subject can file a complaint with the competent authority however it is silent on the filing of appeal by the controllers against the decisions of the competent authority.

47. Are there any identifiable trends in enforcement activity in your jurisdiction?

As the PDPL has yet not been implemented, hence enforcement trends could not be identified.

48. Are there any proposals for reforming data protection laws in your jurisdiction currently under review? Please provide an overview of any proposed changes and the legislative status of such proposals.

No public information is available in this regard.

Contributors

Saifullah Khan
Director
saifullah.khan@drouaalamal.sa

Saeed Hasan Khan
Director
saeed.hasan@drouaalamal.sa