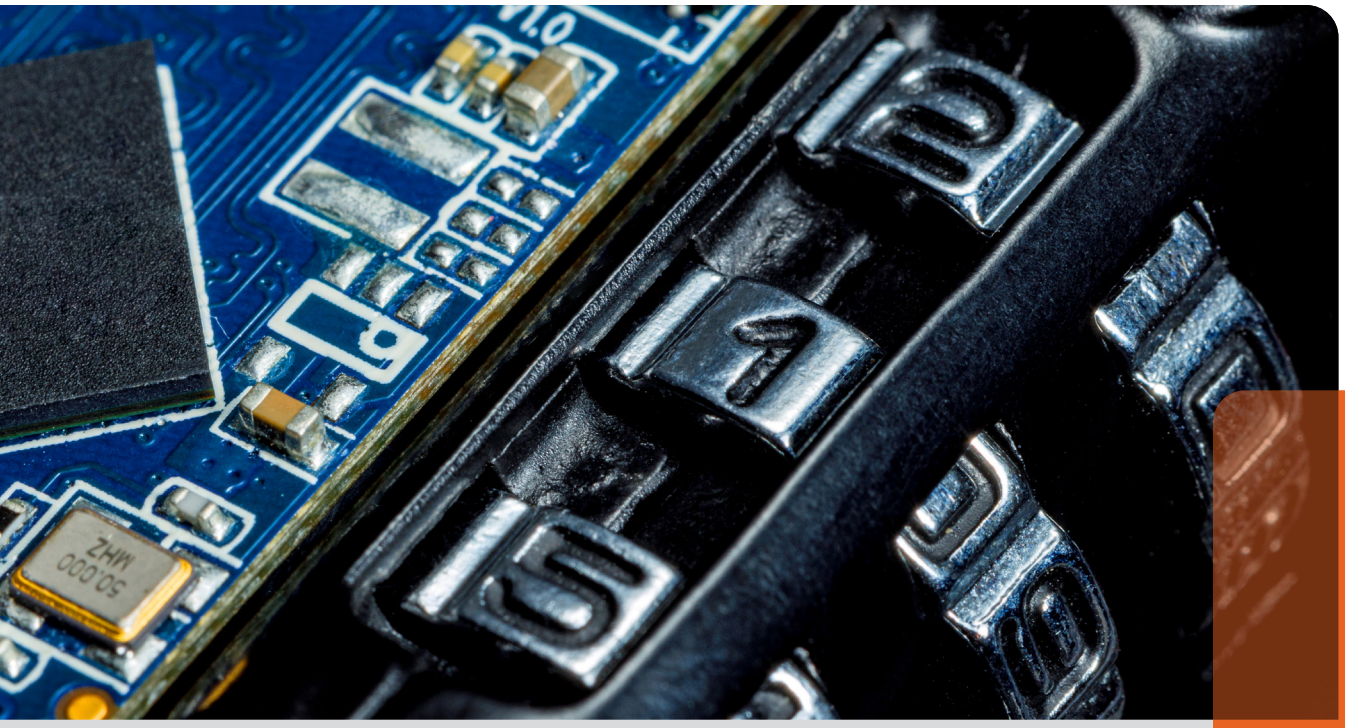
International
Comparative
Legal Guides



Data Protection

2024

11th Edition

Contributing Editors:
Tim Hickman & Detlev Gabel
White & Case LLP

glg Global Legal Group

Expert Analysis Chapters

Q&A Chapters

Saudi Arabia

Saifullah Khan

Saeed Hasan Khan

Droua Al-Amal Consultants

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection law in the Kingdom of Saudi Arabia (the Kingdom) is the Personal Data Protection Law (PDPL), issued pursuant to Royal Decree No. M/19 dated 09/02/1443 AH, corresponding to 16 September 2021. The law was enforced on 14 September 2023; however, a grace period of one year, i.e. until 14 September 2024, has been granted to entities, to comply with the data privacy law.

The implementing regulations of the PDPL have also been issued, which have elaborated the principles of the PDPL. In addition, the Regulation on Personal Data Transfer outside the Kingdom has also been issued, which allows the transfer of personal data outside the Kingdom, subject to certain requirements.

1.2 Is there any other general legislation that impacts data protection?

The Basic Law of Governance (Constitution) at its Article 40 guarantees the privacy of telegraphic and postal communications, and prohibits confiscation of communication. Further, Article 37 of the Basic Law of Governance provides that houses are inviolable; thereby, setting the ground for respect of privacy of individuals.

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

1.3 Is there any sector-specific legislation that impacts data protection?

The following are sector-specific laws relating to data protection:

- The Telecommunication and Information Technology Act.
- The Electronic Commerce Law.
- The Electronic Transactions Law.
- The Law of Practicing Healthcare Professions.
- The Payment Service Provider Regulatory Guidelines issued by the Saudi Central Bank (SAMA).

1.4 What authority(ies) are responsible for data protection?

The Saudi Data and Artificial Intelligence Authority (SDAIA) is the competent authority to supervise the implementation of the provisions of the PDPL. The SDAIA, while exhausting its duties, can request the necessary information and documents from the Controller to ensure compliance with the PDPL and can request cooperation from the other parties as well.

The National Cyber Security Authority has also been established to oversee Cyber Security in the Kingdom.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- "**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, licence numbers, records, personal assets, bank and credit card numbers, photos and videos of an individual, and any other data of a personal nature.
- "**Processing**"
  Any operation carried out on personal data by any means, whether manual or automated, including collecting, recording, saving, indexing, organising, formatting, storing, modifying, updating, consolidating, retrieving, using, disclosing, transmitting, publishing, sharing, linking, blocking, erasing and destroying data.
- "**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.
- "**Data Subject**"
  The individual to whom the personal data relate.
- "**Sensitive Personal Data**"/"**Special Categories of Personal Data**"
  Personal data revealing racial or ethnic origin, or religious, intellectual or political belief; data relating to security, criminal convictions and offences, biometric or genetic

data for the purpose of identifying the person; health data; and data that indicates that one or both of the individual's parents are unknown.

- "**Data Breach**"
  Any incident that leads to the disclosure, destruction or unauthorised access to personal data, whether intentional or accidental, and by any means, whether automated or manual.
- "**Pseudonymisation**"
  Conversion of the main identifiers that indicate the identity of the data subject into codes that make it difficult to directly identify them without using additional data or information. The pseudonymised data or additional information should be kept separately, and appropriate technical and administrative controls should be implemented to ensure that they are not specifically linked to the data subject's identity.
- "**Anonymisation**"
  Removal of direct and indirect identifiers that indicate the identity of the data subject in a way that permanently makes it impossible to identify the data subject.
- "**Vital Interest**"
  Any interest necessary to preserve the life of a data subject.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The PDPL is applicable to any business established in other jurisdictions only if such business is, by any means, processing personal data of individuals residing in the Kingdom; this also includes the personal data of the deceased that would lead to the identification of such deceased individual or specifically their family.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The PDPL will not be applicable to processing that involves the processing of personal data for personal and family usage and does not go beyond it; however, such exemption is applicable only to the extent that the data subject does not publish his/her personal data to third parties. Personal and family use is defined as follows:

Processing personal data, by individuals, within their family or limited social circle as part of any social or family activity. However, the following is excluded from the domain of personal or family use:

- When the personal data is published to the public or is disclosed to any person outside the definition of personal or family use.
- When personal data is being used for professional, commercial or non-profit purposes.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  According to the PDPL, the means and methods used for the processing of personal data must be direct, clear and secure, must not involve any deception and must not mislead or extort the data subject for the processing of personal data.
- **Lawful basis for processing**
  The purpose for which personal data is collected must be legitimate and should not be against any legal provision.
- **Purpose limitation**
  The personal data processed shall be appropriate and limited to the purpose for which it is collected.
- **Data minimisation**
  The Controller shall collect the minimum amount of personal data that is necessary to achieve the purpose for which personal data is being processed.
- **Proportionality**
  Personal data processed must be proportionate to the extent that is necessary for the purpose for which personal data is collected.
- **Retention**
  When the personal data collected is no longer necessary for the purpose for which it was collected, the Controller shall cease their collection without undue delay and shall destroy previously collected personal data at once. However, the Controller may retain the personal data after completion of the purpose of collection, when the personal data processed does not contain anything that may lead to specifically identifying the data subject. In addition, the Controller may also retain the personal data in the following cases:
  - When there exists a legal basis for retaining personal data for a specific period of time; however, such personal data must be destroyed once the time period lapses or when the purpose of collection is satisfied, whichever is longer.
  - When the personal data processed is relevant with a case that is *sub judice* before a judicial authority, in such circumstances the personal data can be retained; however, once the judicial procedures are concluded, the Controller must destroy the personal data.
- **Accuracy**
  The personal data processed must be accurate, complete and relevant to the purpose for which it is collected.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of Information**
  The data subject has a right to be informed of the legal basis and purpose of the processing of personal data. The following information, before or at the time of collection of personal data, is to be given to the data subject:
  - The identity of the Controller, including contact details and details related to the channels developed by the Controller for the data subject to have communication regarding protection of personal data.
  - Contact details of the Data Protection Officer (DPO), when appointed.
  - The legal basis and a clear, specific and explicit purpose of the processing of personal data.
  - The duration the personal data will be kept. In case determining the period of retention is not possible, the data subject is to be informed about the criteria used to determine the retention period.
  - Rights available to the data subject and the procedure to exercise the rights.

- The procedure to withdraw consent.
- Whether it is mandatory or optional to collect/process the personal data.

- **Right of access to (copies of) data/information about processing**
  The law has given this right to the data subject that he/she can request for the copy of their personal data processed in a readable and clear format, on request by the data subject or without request by the data subject through a channel provided by the Controller, enabling the data subject to have access to the personal data.
  While requesting access to and copies of the personal data, the data subject is subject to the following conditions:
  - Exercise of such right, i.e. to access personal data, should not have any adverse effect on the rights of others, such as intellectual property rights or trade secrets.
  - Personal data is to be provided in a commonly used electronic format and the data subject may ask for a printed copy if feasible.
  - While granting access to the data subject to their personal data, the Controller must ensure that the data being disclosed does not involve any such data that identifies another individual.
- **Right to rectification of errors**
  The data subject has the right to request correction, completion or updating of personal data. In this regard, the Controller may request required evidence to verify the request of the data subject. The evidence, so provided by the data subject, must be destroyed once the verification process is completed.
  After the correction of the personal data, the Controller shall, without undue delay, notify the parties to whom the personal data was previously disclosed.
- **Right to deletion/right to be forgotten**
  The data subject can request the destruction of the processed personal data. The Controller is under obligation to destroy personal data in the following circumstances:
  - When the data subject has made a request for the personal data to be destroyed.
  - When the personal data is no longer necessary for the purpose it was collected.
  - If the data subject withdraws his/her consent for the processing of the personal data and the consent is the sole legal basis for processing.
  - If it comes into the Controller's knowledge that personal data is being processed in a manner that violates the PDPL.

  While destroying personal data, the Controller must be considerate of the following:
  - The Controller must take appropriate measures to notify the other parties with whom the Controller had shared the data and must request for the personal data to be destroyed.
  - The Controller must notify any individual with whom the personal data has been shared by any means about the destruction of the personal data by the Controller and will request for him/her to do the same.
  - The Controller must destroy all copies of the personal data stored in the Controller's systems, including any backups, in accordance with the applicable regulatory requirements.
- **Right to object to processing/Right to restrict processing**
  A data subject can request the Controller to restrict processing in case the data subject has contested authenticity of the personal data processed by the Controller, and request for its correction. Such restriction period must enable the Controller to have a time period during which the Controller must verify the accuracy of the personal data.
- **Right to withdraw consent**
  The data subject has the right to withdraw their consent for the processing of their personal data at any time. The data subject is to inform the Controller of such withdrawal through any available means in accordance with the Regulations.
- **Right to object to marketing**
  The data subject has the right to opt for not receiving marketing materials. When a Controller has to process personal data for direct marketing purposes, it must obtain consent from the data subject. Also, the Controller must devise a mechanism that enables the data subject to opt out of receiving marketing materials.
- **Right to complain to the relevant data protection authority(ies)**
  The data subject may complain to the competent authority after becoming aware of any incident necessitating to make a complaint. The complaint must be filed within a period not exceeding 90 days from the date when the matter has come into the data subject's knowledge.
- **Other key rights**
  The PDPL, besides laying down the penalties for the Controllers/Processors with respect to the violation of the PDPL, also gives a right to the data subject to file for compensation. An individual that suffers damage as a result of any of the violations stated in the PDPL or regulations may apply before a competent court of law for proportionate compensation for the material or moral damage.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

There is no such right under the PDPL.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

The PDPL enables a legal guardian to act on behalf of a data subject that partially or fully lacks the legal capacity. The PDPL requires the legal guardian to act in the best interests of the data subject, which may be a child in this case and for this purpose the PDPL has entrusted the legal guardian with two of the following options:

- On behalf of the data subject, the legal guardian can exercise the rights granted to the data subject (child) under the PDPL.
- The legal guardian can give consent on behalf of the data subject (child) for the processing of the personal data; however, the obtaining of the consent of the legal guardian is conditional upon the measures to be put in place to verify the validity of guardianship of the legal guardian over the data subject.

While obtaining the consent from the legal guardian on behalf of the data subject (child), the Controller must be cautious of the following:

- This process shall not cause any harm to the interest of the data subject.
- It shall enable the data subject to exercise their rights as per the PDPL.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

The PDPL, while providing powers of the competent authority (SDAIA), empowers the SDAIA to specify the appropriate tools and mechanism to monitor compliance of the Controllers with the PDPL. These tools and mechanism may also include maintenance of a national register of Controllers.

The SDAIA is to issue rules for registration in the referred national register, including which Controllers need to be registered.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Rules for registration have not yet been issued.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Rules for registration have not yet been issued.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Rules for registration have not yet been issued.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Rules for registration have not yet been issued.

7.6 What are the sanctions for failure to register/notify where required?

Rules for registration have not yet been issued.

7.7 What is the fee per registration/notification (if applicable)?

Rules for registration have not yet been issued.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

Rules for registration have not yet been issued.

7.9 Is any prior approval required from the data protection regulator?

Rules for registration have not yet been issued.

7.10 Can the registration/notification be completed online?

Rules for registration have not yet been issued.

7.11 Is there a publicly available list of completed registrations/notifications?

Rules for registration have not yet been issued.

7.12 How long does a typical registration/notification process take?

Rules for registration have not yet been issued.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of the DPO is mandatory in the following circumstances:

- If the Controller is a public entity and is involved in the processing of the personal data on a large scale.
- The primary activities of the Controller involve the carrying out of such processing operations that require regular and continuous monitoring of individuals on a large scale.
- The Controller's core activities consist of processing sensitive personal data.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

There is no dedicated/specified penalty for failing to appoint a DPO. Such failure being a violation of the PDPL, general penalties like a warning or a maximum fine of up to Saudi Riyals five million may be imposed. In case of repetitive violation, the fine may be doubled.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The PDPL is silent on this matter.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

The PDPL is silent on this matter. The competent authority (SDAIA) is to issue rules for the appointment of a DPO. It is likely that such matters will be dealt with/clarified in the rules to be issued.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The DPO may be an official, an employee or an external service provider of the Controller. The PDPL does not mention any specific qualification for the DPO. The competent authority (SDAIA) is to issue rules for the appointment of a DPO. It is likely that such matters will be dealt with/clarified in the rules to be issued.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Broadly, the DPO must monitor the implementation of the provisions of the PDPL and oversee the methods adopted by the Controller in order to comply with the PDPL and manage data subject requests.

The specific functions of the DPO include:

- To act as a point of contact between the competent authority and the Controller and to comply with the competent authority's decisions and instructions with respect to the application of the PDPL and its regulations.
- To supervise the following procedures and issue necessary recommendations accordingly:
  - i) impact assessments;
  - ii) audit reports;
  - iii) evaluations related to personal data protection controls; and
  - iv) documentation of assessment results.
- To enable the data subjects to exercise their rights as given under the PDPL.
- To notify the competent authority with respect to any incident of a personal data breach.
- To respond back to requests made by data subjects and also to address complaints submitted by the data subjects.
- To maintain and update the record of the processing activities of the Controller.
- To address any violations of the PDPL made by the Controller and to take the corrective measures.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The PDPL does not set any such requirement. However, it is likely that the rules to be issued by the competent authority (SDAIA) may contain such requirement.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

As part of the rights conferred on the data subjects (right to be informed), the Controller is to inform the contact details of the DPO to the data subjects.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

While appointing the processor for the processing on behalf of the Controller, the Controller shall ensure that the appointed processor must provide sufficient guarantees to comply with the PDPL and its implementing regulations. The Controller, in this regard, must conclude an agreement with the processor. Such guarantees, however, do not dilute the obligations of the Controller towards the data subject or the competent authority.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

It is necessary to enter into an agreement with the processor. The agreement must provide the following:

a) The purpose for which the personal data is to be processed.
b) The categories of the personal data being processed.
c) The duration for which the processing will take place.
d) The processor's commitment to notify the Controller of any breach incident, in accordance with the provisions of the PDPL.
e) Clarification from the processor that similar laws (equivalent to the PDPL) in other jurisdictions are applicable on its impact on the processing.
f) That the processor need not to obtain the data subject's prior consent for mandatory disclosure of personal data under the applicable laws in the Kingdom; however, the processor must notify the Controller of any such disclosure.
g) The processor shall identify any sub-contractors to be appointed by the processor, or any other party with whom the personal data shall be shared.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The public entities may use personal means of communication (post and email) for sending awareness-raising material. However, the Controller may not use personal means of communication, including post and email, unless it fulfils certain conditions. Before sending awareness-raising material, the Controller must:

- obtain consent of the recipient; and
- provide a clear mechanism to enable the recipient to opt out of receiving such awareness material.

In addition to the applicable requirements under the Telecommunication and Information Technology Act, the Controller is further to observe the following:

- To clearly show the identity of the sender.
- To provide a mechanism enabling the data subject to opt out and to ensure that the relevant procedure to opt out is as easy as to give consent.
- To immediately stop sending materials as soon as the recipient asks to opt out.
- To stop sending the material without any fee.
- To preserve the consent received from the recipient.

Apart from the above, the Controller (with the exception of sensitive data) may process personal data for marketing purposes by observing the following controls:

- Obtaining the consent of the data subject.
- Providing a mechanism enabling the data subject to opt out and to ensure that the relevant procedure to opt out is as easy as to give consent.

- Clearly state the identity of the sender without any anonymisation.
- Immediately stop sending marketing materials as soon as the data subject withdraws his/her consent.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The PDPL does not draw any differentiation, in the context of business-to-consumer or business-to-business marketing, as regards the above-mentioned controls.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

As explained at question 10.1 above.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

As the PDPL is applicable to Controllers outside the Kingdom (due to extra-territorial applicability), the controls mentioned above do apply on marketing sent from other jurisdictions.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

There is a grace period (until 14 September 2024) for implementation of the PDPL; therefore, at the time of writing, there are insights on the enforcement actions.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

The PDPL is silent on this particular matter; however, this seems against the very principles of the PDPL unless consented by the data subjects.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

There is no dedicated/specified penalty for sending marketing communications in contradiction of the requirements of the PDPL. Such contradiction being violation of the PDPL, general penalties like a warning or a maximum fine of up to Saudi Riyals 5 million may be imposed. In case of repetitive violation, the fine may be doubled. In case sensitive data is the subject matter of any marketing, the maximum penalty is Saudi Riyals 3 million or imprisonment for up to two years, or both.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The PDPL is silent on the use of cookies.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The PDPL is silent on the use of cookies.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The PDPL is silent on the use of cookies.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

The PDPL is silent on the use of cookies.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

A Controller may transfer personal data outside the Kingdom or may disclose it to a party outside the Kingdom in order to achieve the following purposes:

a) If the data to be transferred is related to performing an obligation under an agreement to which the Kingdom is party.
b) If such transfer of personal data would serve the interest of the Kingdom.
c) If the transfer of the personal data is with respect to the performance of an obligation.
d) If the transfer is for the purposes as mentioned in the regulations (Regulation on Personal Data Transfer outside the Kingdom).

Conditions to be met for the transfer of the personal data:
While transferring personal data outside the Kingdom, the Controller must consider the following conditions:

- The transfer or disclosure of personal data shall not cause any prejudice to national security or vital interests of the Kingdom or violate any other law of the Kingdom.
- The Controller must limit the transfer or disclosure of the personal data outside the Kingdom, i.e. only the minimum data must be transferred that is necessary to achieve the purpose of the disclosure/transfer.
- Ensure there is an adequate level of protection for personal data outside the Kingdom. There must be at least similar protection, outside the Kingdom, as is available under the PDPL in accordance with the assessment carried out by the competent authority.

While transferring personal data outside the Kingdom, the Controller must ensure that the disclosure/transfer does not impact the privacy of the data subjects or does not impact negatively the level of protection guaranteed under the PDPL. Considering these points, the Controller must ensure that the following aspects are not compromised:

a) The data subject's ability to exercise their rights as conferred by the PDPL.
b) The data subject's ability to exercise their right to withdraw their consent to the processing.
c) The Controller's ability to comply with requirements for notifying personal data breaches.

d) The Controller's ability to comply with provisions, controls and procedures for disclosing personal data.
e) The Controller's ability to comply with provisions and controls for destroying personal data.
f) The Controller's ability to take necessary organisational, administrative and technical measures to ensure the security of the personal data.

In the absence of an adequate level of protection, the personal data may be transferred by way of the following appropriate safeguards:

- Binding Common Rules (as approved by the competent authority).
- Standard Contractual Clauses (as issued by the competent authority).
- Certification of Compliance by an entity authorised by the competent authority.
- Binding Codes of Conduct (as approved by the competent authority).

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Currently, due to the grace period (up to 14 September 2024) the provisions of the PDPL are not being implemented/enforced; therefore, no such information is publicly available. On the face of it, consent of the data subject and performance of a contract with the data subject seems more convenient over other options.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

As mentioned at question 12.1, the Binding Common Rules, Standard Contractual Clauses and Binding Codes of Conduct must be issued/approved by the competent authority.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

The Controller must conduct a risk assessment for the transfer of personal data outside the Kingdom or disclosure to a party outside the Kingdom in any of the following cases:

- When the transfer of the personal data outside the Kingdom is based on appropriate safeguards.
- When the appropriate safeguards for transfer of personal data outside the Kingdom are not required.
- When continuous or large-scale transfer of sensitive personal data is to be carried out outside the Kingdom.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

This is not applicable.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

There is no guidance on the use of standard contractual/model clauses.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

On 13 February 2024, a new law for the Protection of Whistle blowers, Witnesses, Experts and Victims was published. The said law provides for the court to protect individuals who give evidence from being intimidated that may cause impact on their testimony, including whistleblowers, other witnesses, experts and victims. Protection includes removing their name and address from any correspondence, documents and minutes, concealing them while giving evidence in court or permitting them to give evidence behind closed doors. Based upon the said law, the establishment of the Centre for the Protection of Whistleblowers, Witnesses, Experts, and Victims has also been approved.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is generally permitted.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

A law relating to the use of surveillance cameras in the Kingdom is made *vide* Royal Decree No. 164 dated 7 October 2022 (the KSA Surveillance Cameras Law). The KSA Surveillance Cameras Law makes it mandatory to install surveillance cameras in public places like ministries, commercial complexes, health care facilities, financial institutions, etc. The KSA Surveillance Cameras Law states that installing, operating or maintaining security surveillance cameras is not permissible except with the approval of the Ministry of Interior.

14.2 Are there limits on the purposes for which CCTV data may be used?

As mentioned at question 14.1.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

The PDPL is silent on employee monitoring.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

The PDPL does not create any exception as regards the processing of personal data of employees or otherwise. Therefore, consent is required unless specifically excluded. The most typical mode to obtain consent from employees is through an employment agreement.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Trade unions are not permitted in the Kingdom.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

There is no specific restriction to process an employee's attendance in office.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

The Controller shall take the necessary organisational, administrative and technical measures to ensure the security of personal data and the privacy of data subjects. For security purposes, the Controller must comply with the following:

- Implement necessary security and technical measures to limit security risks related to a personal data breach.
- Comply with the relevant controls, standards and rules issued by the National Cybersecurity Authority or recognised best practices and cyber security standards if the Controller is not obligated to follow the controls, standard and rules issued by the National Cybersecurity Authority.

The Controller, while appointing a processor, shall ensure that the chosen processor provides sufficient guarantees to protect the personal data.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

When a data breach incident will potentially cause harm to the personal data or to the data subject, or conflicts with the data subject's rights and interests, the Controller shall notify the authority within a time period not exceeding 72 hours of becoming aware of the incident. If the Controller fails to notify the authority within the prescribed time after it became aware of the breach incident, then it shall provide the requisite information to the authority as soon as possible, along with a justification of delay. The Controller must also keep a copy of the report submitted to the authority and must document the corrective measures taken in relation with the personal data breach, as well as any relevant documents or supporting evidence.

The data breach notification shall include the following information:

a) A description of the personal data breach incident, which includes the time, date and circumstances of the breach and the time when the Controller became aware of the breach.
b) The categories of data impacted by the breach, actual or approximate numbers of impacted data subjects and the type of personal data effected by the breach incident.
c) A description of the risks of the personal data breach, including the actual or potential impact on personal data and data subjects, and the actions and measures taken by the Controller after the breach to prevent or limit the impact of those risks and to mitigate these risks. Also a description of the future measures that will be taken to avoid a recurrence of the breach.
d) A statement of the Controller wherein it states whether the data subject has been notified of the breach incident.
e) Contact details of the Controller or any DPO, if appointed, or any other official who has knowledge of the reported incident.

The provisions of the PDPL do not prejudice the obligations of the Controller or Processor as conferred by the National Cybersecurity Authority, relevant to the personal data breach notification.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

When an incident of personal data breach may cause damage to the data subject's personal data or may conflict with their rights or interests, the Controller must notify the data subject of such incident of breach without undue delay (i.e. within 72 hours); furthermore, the language of the notification must be simple and clear. The personal data breach to be notified to the data subject must include the following information:

- A description of the personal data breach.
- A description of the potential risks that may arise from the personal data breach.
- A description of the measures taken to mitigate the potential risks that may arise from the personal data breach.
- The name and contact details of the Controller, as well as the contact details of any DPO appointed; moreover, any appropriate means of communication with the Controller.
- The notification shall contain a recommendation or advice that may assist the data subject in taking appropriate measures to safeguard against the identified risks or to mitigate the impact of the potential risks.

16.4 What are the maximum penalties for personal data security breaches?

Any individual who violates the provisions of the PDPL by disclosing or publishing sensitive personal data, with the intention of harming the data subject or achieving any personal motive, shall be punished with an imprisonment for a period not exceeding two years or a fine not exceeding Saudi Riyals 3 million, or both.

Apart from the above, any other violation of the PDPL attracts the issuance of a warning, or a maximum fine of up to

Saudi Riyals 5 million may be imposed. In case of repetitive violation, the fine may be doubled.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

(a) **Implementation:** The SDAIA, being the competent authority, has the mandate to oversee the implementation of the PDPL and its implementing regulations.
(b) **Calling for Documents or Information:** The SDAIA is empowered to ask the Controllers for the necessary documents or information to ensure compliance of the PDPL.
(c) **Asking Cooperation:** The SDAIA may request any party to cooperate to support the accomplishment of its enforcement functions under the PDPL.
(d) **Specification of Tools:** The SDAIA may, in order to monitor compliance by the Controllers, specify the appropriate tools and mechanism, including maintaining a national register of Controllers.
(e) **Service Provision:** The SDAIA may, through the referred national register, provide services related to personal data protection.
(f) **Complaints Processing:** The SDAIA is empowered to receive and to take actions on the complaints of the data subjects.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

This power is not mentioned in the PDPL.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The PDPL, due to having a grace period, has not been implemented; therefore, there have been no examples of exercise of the powers of the SDAIA.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The PDPL, due to having a grace period, has not been implemented; therefore, there have been no examples of exercise of the powers of the SDAIA.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

The PDPL is silent on this aspect. However, generally, the foreign law enforcement agencies do not communicate with businesses directly; rather, businesses are contacted via the relevant law enforcement agencies of the Kingdom, who coordinate with businesses to respond to foreign law enforcement agencies.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

No guidance has been issued.

19 Trends and Developments

19.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

The PDPL, due to having a grace period, has not been implemented; therefore, there are no enforcement trends.

19.2 What "hot topics" are currently a focus for the data protection regulator?

The 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.

Saifullah Khan is an international trade, privacy and policy lawyer with more than 20 years of diversified and multi-jurisdictional professional experience serving a large client base in the domestic and international markets. His areas of interest include trade remedy laws of the World Trade Organization, customs law, competition law and data privacy. With respect to emerging discipline of data privacy, he advises clients from different jurisdictions on data privacy compliance and cross-border transfer of data. Additionally, he assists clients in the preparation and review of privacy policies and intra-group agreements concerning cross-border transfer of personal data, etc. He is an advocate of the High Court, a member of the Chartered Institute of Arbitrators (UK) and a member of the International Association of Privacy Professionals. He has completed a course at the London School of Economics and Political Science on "Data: Law, Policy and Regulation".

Droua Al-Amal Consultants
7289-7207 Wadi Taraj
An Nakheel Riyadh 12381
Saudi Arabia

Tel: +966 53 069 2265
Email: saifullah.khan@drouaalamal.sa
LinkedIn: www.linkedin.com/in/saifullahkhan

Saeed Hasan Khan has vast experience advising clients on various issues such as taxation, corporate, regulatory compliance, contractual obligations, etc. and representing them before the authorities. Over the past 20 years, he has practised in direct and indirect taxes, which encompasses all three practice tiers: advisory; execution; and litigation. He advises on cross-border transactions, international tax treaties and matters related to tax due diligence, corporate structures, shareholder agreements and contractual stipulations between the companies. He has developed a keen professional interest in emerging laws about personal data protection and has gained a deep understanding of underlying concepts and principles governing the global data protection laws including the General Data Protection Regulation of the European Union.

He carried out a great deal of research on personal data protection laws in various jurisdictions to have a comparison of core legal principles in a range of jurisdictions. He attended a course at the London School of Economics and Political Science on "Data: Law, Policy and Regulation". He is an Advocate of the High Court, a Member of the Chartered Institute of Arbitrators (UK) and a Member of the International Association of Privacy Professionals.

Droua Al-Amal Consultants
7289-7207 Wadi Taraj
An Nakheel Riyadh 12381
Saudi Arabia

Tel: +966 53 906 2286
Email: saeed.hasan@drouaalamal.sa
LinkedIn: www.linkedin.com/in/saeedhasankhan

Droua Al-Amal Consultants carries the rich, multi-faceted and multi-jurisdictional experience, spreading over two decades, of its directors. The company endeavours to be a professional service provider, which synthesises the learning from a vast experience-base and converts that into advantage for its clients. The services we offer, to our prestigious clients, are based on profound industry and legal knowledge.

www.drouaalamal.sa

DROUA
شركة ذروة الاعمال للاستشارات المهنية
Droua Alamal For Consultancy Services

International Comparative Legal Guides

The **International Comparative Legal Guide** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

Data Protection 2024 includes two expert analysis chapters and 31 Q&A jurisdiction chapters covering key issues, including:

- Relevant Legislation and Competent Authorities
- Definitions
- Territorial and Material Scope
- Key Principles
- Individual Rights
- Children's Personal Data
- Registration Formalities and Prior Approval
- Appointment of a Data Protection Officer
- Appointment of Processors
- Marketing
- Cookies
- Restrictions on International Data Transfers
- Whistle-blower Hotlines
- CCTV
- Employee Monitoring
- Data Security and Data Breach
- Enforcement and Sanctions
- E-discovery/Disclosure to Foreign Law Enforcement Agencies
- Trends and Developments

The International Comparative Legal Guides are published by: glg Global Legal Group