| | |
|---|---|
| Article 2 | Scope of the law: the PDPL applies to all processing in the KSA and to all individuals living in the KSA (even if the processor is an entity present abroad).<br>The PDPL includes deceased individuals' personal data, unlike other international data protection laws |
| Article 3 | This article states that the most "protective" legal regime for personal data applies (judiciary decision, other legal regime, international treaty that KSA is part of). |
| Articles 4-5 | Data Subject Rights: Data subjects will have the right to be **informed** of personal data processing and the legal basis for such processing, the right to access their personal data (including the right to obtain a free copy), the right to correct or update their personal data, and the right to request its destruction if it is no longer needed, subject to some exceptions. Data subjects can also file complaints with the regulatory authority about how the PDPL is being implemented.<br>Data subjects have the right to withdraw their consent to personal data processing at any time. |
| Article 6 | **Non-consent based processing:** Regardless of the provisions related to withdrawal of consent, the PDPL makes it clear that data processing does not always necessitate the data subject's consent.<br>Consent is not required:<br>- if the processing would result in a clear benefit for the data subject and if contacting the data subject seems impossible or impractical<br>- if the processing is required by law or a prior agreement to which the data subject is a party<br>- if the controller is a public entity and the processing is required for security or judicial purposes.<br>(Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data) |
| Article 8 | The Controller has to make sure that:<br>- Data processor chosen should be able to guarantee the application of laws and regulations<br>- Data processor follows orders and guidelines given by the controller when it comes to the protection of personal data<br>- Data processor is responsible towards the supervising authority and towards the data subject. |
| Article 9 | The right of access to personal data could be restricted (in time) by the controller if:<br>- it's necessary to protect the data subject's personal data or any other individual from prejudice<br>- If the controller is a state entity (public entity) restricting the right of access for security purposes or to comply with a different framework or |

| | |
|---|---|
| | even for judicial purposes.<br>The same restrictions apply in the GDPR in its article 23 but the GDPR provides more exceptions and provisions to limit the right of access to personal data. |
| Article 10 | Data collection should be direct: from the data subject<br>**Indirect collection of personal data** is accepted in the law but in certain restricted cases only. Such collected data may be processed for a different purpose than the one for which it was collected. Article 10 lists the cases where this is lawful. |
| Article 11 | The purpose of processing personal data must be related to the controller's "business" and must not be contrary to other regulations.<br>Data Collection must not be contrary to any regulations and free from fraud, misrepresentation or extortion<br>The data collection must be limited to the *least possible*.<br>After the collected data is not necessary anymore, data collection should be stopped and the data already collected must be deleted. |
| Article 12 | Controllers must, in the PDPL, implement a privacy policy and make it available to data subjects prior to collecting personal information from them. The PDPL specifies the minimum amount of information that must be included in a privacy policy, including when personal data is collected directly from the data subject. |
| Article 13 | This article cites the different information that should be given to a data subject prior to data processing: the legal framework, the legitimate ground for processing, the controller's identity and address (except if the processing is for security reasons), identity of data processors, third parties who have access to data, the risks of the processing, the data subject's rights, etc. |
| Article 14 | The Controller should ensure the data collected is accurate, complete, up to date and linked to the legitimate ground for processing. |
| Article 15 | This article cites the cases where the controller should communicate the collected personal data:<br>1. Consent of the data subject<br>2. If the data is part of the public domain<br>3. If requested by an official authority for security purposes or to comply with a different framework or even for judicial purposes.<br>4. If it's necessary to protect public order, public health, one's life or one's health.<br>5. If the data does not allow the identification of an individual. |
| Article 16 | Exceptions (1), (2) and (5) from Article 15 do not apply in certain cases, most notably:<br>- If this communication would result in damage to the Kingdom's reputation or interests or if it would constitute a danger to security |

| | |
|---|---|
| | - If it would impact the Kingdom's diplomatic relations<br>- If this communication would reveal the existence of a confidential source of information that should not be disclosed for public interest.<br>Etc. |
| Article 17 | Right to modify/alter/correct data and the deadlines to do so. |
| Article 18 | After the purpose of the processing is completed, the controller is **required** to erase personal data. In certain circumstances, it may be able to retain de-identified data or personal data required to be retained by law or in legal proceedings.<br><br>In the GDPR, in its Article 5, the controller can retain data for a specific period of time and it is up to the controller to determine this period. In the GDPR, the controller may retain the personal data collected when the data still has an administrative interest for the organization or when it is a legal obligation. The data can even be archived. But, both of these steps require an evaluation. |
| Article 19 | Due diligence of the controller when it comes to protecting personal data. |
| Article 20 | **Data breaches:** leakages or unauthorized access to personal data must be reported to the supervising authority immediately, and incidents that cause material harm to the data subject must be reported to the data subject.<br><br>The provisions for notification of violations are stricter than those in many international laws, including the GDPR, with a requirement for "immediate" notification rather than within a specified period. Executive regulations supplementing the law should also be issued within this time frame. (This deadline may be extended for certain entities). (Articles 33-34 of the GDPR) |
| Article 21 | The controller must answer the requests of the data subject related to the data subject's rights in a determined duration and through a medium determined by the decrees. |
| Article 22 | **Impact assessments:** Controllers must assess the impact of processing personal data and, if personal data is no longer required to achieve the intended purpose, the controller must stop collecting such data. |
| Article 23 | **Specific provisions for health data**: It is necessary to restrict the right of access to health data - including medical records - to the smallest possible number of employees or workers and only to the extent necessary to provide the necessary health services. It is also necessary to restrict the procedures |

| | |
|---|---|
| | and operations for processing health data to a minimum number of employees and workers for the provision of health services or health insurance programs.<br><br>There is no mention of a specific certification for health data stocking just like the Hébergeur de Données de Santé certification in European Law. |
| Article 24 | **Specific provisions for credit data:** Steps must be taken to verify the availability of the written consent of the owner of the personal data to collect such data or to change the purpose of its collection, disclosure or publication in accordance with the provisions of the system and the credit information system. The Controller has an obligation to inform the owner of the personal data when a request for disclosure of his or her credit data is received from any party. |
| Articles 25-26 | Personal data can be used for marketing purposes, but there are rules in place. This means that data controllers must not use the data subject's personal communications, including postal and electronic addresses, to send promotional or awareness materials without first obtaining the data subject's consent and providing the data subject with an opt-out mechanism.<br><br>Same principles apply in the GDPR. |
| Article 27 | Data Processing without consent for research or statistics purposes is allowed if the data collected:<br><br>- If the data is de-identified<br>- What can identify the subject is deleted before communicating the data (excluding sensitive data)<br>- If this processing is governed by other laws/regulations or by an agreement where the data subject is party.<br><br>The GDPR, on the other hand, allows processing without consent for "legitimate interests". Research is not explicitly designated as its own lawful basis for processing, but it may qualify as a legitimate interest of the controller under Article 6(1)(f) in some cases. Thus, while the GDPR expressly permits re-purposing collected data for research purposes, it may also permit a controller to collect personal data for research purposes without requiring the data subject's consent. |
| Article 28 | Is it not allowed to copy official documents that determine the data subject's identity. It is allowed only to enforce a court decision or if a public authority demands it. |

| | |
|---|---|
| Article 29 | **Data sovereignty:**<br><br>Data controllers can not transfer personal data outside of Saudi Arabia, except:<br><br>- as necessary to comply with an agreement to which the Kingdom is a party<br>- to further Saudi interests<br>- for other purposes to be set forth in executive regulations.<br>- It will also be necessary to ensure that the transfer or disclosure of the data to a party outside the Kingdom does not impact national security or Saudi interests<br>- The controller needs to obtain approval from the Saudi Authority for Personal Data and Artificial Intelligence.<br>- Furthermore, with respect to the disclosure of personal data, caveats are considered if disclosure may pose a security risk, damage the reputation of the Kingdom or impact Saudi Arabia's relations with other countries.<br><br>Data transfers outside the EU are regulated in the GDPR by articles 44 to 50. Chapter 5 of the GDPR specifies two conditions under which data transfers outside the EU/EEA are permitted:<br><br>- Where the European Commission has determined that a third-country has adequate data protection laws.<br><br>- In the absence of an adequate decision. It is up to the data controller and processor to reach an agreement that protects data subjects' rights and remedies in the same way that the regulation does.<br><br>This point could be questionable in an environment where data transfers could easily be justified by regulations like the American Cloud Act *("The CLOUD Act allows American law enforcement to compel U.S.-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data is stored in the U.S. or on foreign soil, and attempts to resolve a long-running legal battle between 'big tech' and law enforcement.")*, especially given the number of American companies handling cloud computing from KSA (AWS, Google). This is also a debate in the European Union.<br><br>The Saudi Data Protection Law takes a stricter approach to data sovereignty |
| Article 30 | This article states that the supervising authority is the authority to supervise the implementation and application of this law. The controller and the supervising authority should work together to make sure the PDPL is being |

| | |
|---|---|
| | applied. The supervising authority can demand of the controller, documents and proof to verify compliance with the PDPL.<br><br>The Controller should appoint a Data Protection Officer to supervise the compliance with the PDPL. |
| Articles 31-32 | **Controller registration:**<br><br>Entities that collect personal data and determine its purpose and method of processing (controllers) will be required to register on an electronic portal that will form a national record of controllers. There will be an annual registration fee that will be determined by executive regulations (which are to be issued in due course).<br><br>Controllers will also have obligations when it comes to the accuracy, completeness and adequacy of personal data prior to processing, to keep a record of processing for a period to be prescribed by the Executive Regulation, and to ensure that staff receive adequate training on the PDPL and data protection principles. |
| Articles 32-33-34 | **Supervising authority:**<br><br>The entity that will be responsible for monitoring/overseeing compliance with this law, sanctioning its violations and before which the persons concerned can make complaints to assert their rights.<br><br>If an entity is processing data from outside of KSA, it should appoint a representative within KSA. The supervising authority should approve and license the representative.<br><br>However, the implementing decree provides that: The requirement for entities located outside the Kingdom that process the personal data of Saudi residents to designate a representative in the Kingdom and comply with the PDPL will be delayed for up to five years from the effective date (to be determined by the SDAIA).<br><br>Data subjects can file a complaint in front of the supervising authority related to the application of the law. |
| Articles 35 to 40 | **Sanctions:**<br>The disclosure/publication of sensitive data in violation of the PDPL can result in up to two years in prison or a fine of up to SAR 3,000,000 (US$ 800,000). Violations of the data transfer provisions may result in up to a year in prison and a fine of up to SAR 1,000,000 (US$ 266,600). All other provisions of the |

| | |
|---|---|
| | PDPL are punishable by a warning notice or a fine of up to SAR 5,000,000 (US$ 1,333,000).<br>For repeat offenses, any of the fines could be doubled, and the court could order confiscation of funds obtained as a result of breaking the law, as well as publication of the judgment in a newspaper or other media at the offender's expense.<br><br>Victims of the crimes may be eligible for restitution. |
| Article 41 | Any individual who took part in the data processing should respect the privacy related to this data even after the processing is over/their job is over. |
| Article 42 | Application decrees will be published in a maximum of 180 days after the publication of the law. |
| Article 43 | This law will be applicable 180 days after it’s published in the official gazette. |