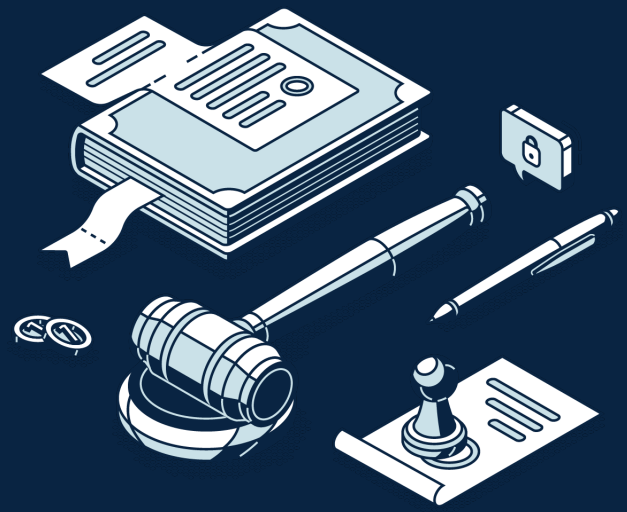
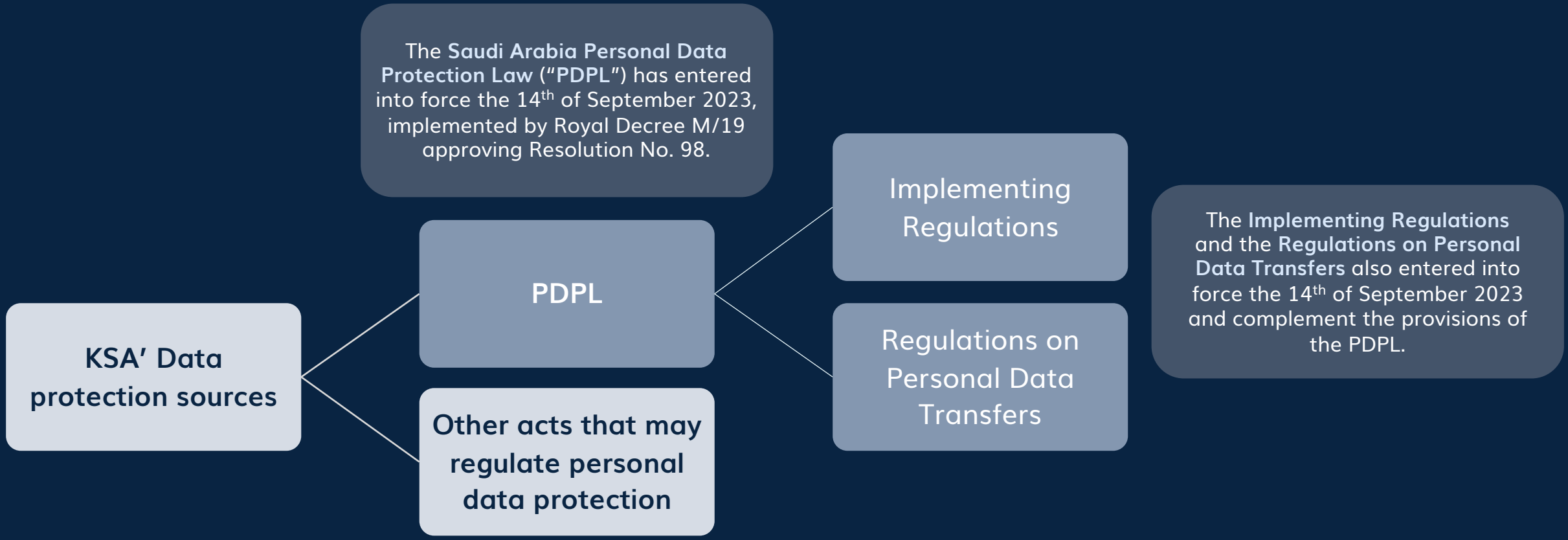
White Label Consultancy

# KSA takes on personal data protection

Key similarities and differences comparing to GDPR you should know about



# KSA Data Protection Landscape



# Key Concepts & Issues

| | Definitions and concepts | Data Breach | Privacy Policy | Privacy Assessments | DPO | Transfer |
|---|---|---|---|---|---|---|
| **Major similarities: GDPR v. PDPL** | Similarly understood definitions of Data, Processing, Processor, Controller, Transfer, Data Subject.<br><br>Uses the same concepts as RoPA, DPO, family use exception. | 1) 72 hours to notify DPA about a breach<br>2) The controller must provide DPA with details of the breach (e.g., description, risks identified, actions / measures taken);<br>3) The controller must notify the data subjects without undue delay if certain conditions are met. | Should specify:<br>• **Legal basis**<br>• Purpose of **collection** and<br>• **Information about the Data Subject rights and how to exercise them**<br>• **Recipients**<br>• **Consequences of not providing the data by the data subject** | Should be carried out if certain conditions are met.<br><br>Both mandate to do an Assessment if the processing re. processing data on large scale or monitoring data subjects | Provide certain conditions which – if satisfied – oblige controllers to appoint a DPO. | Similar transfer mechanisms as: adequacy decisions; standard contract clauses; BCRs.<br><br>Transfer Impact Assessment as a required component of the process. |
| **Major differences under PDPL** | PDPL also introduces **some specific definitions**, such as:<br>1) Credit Data<br>2) Health Data<br>3) Health Services<br>4) Publishing. | | 1) Also, it should specify **Personal Data to be collected, which data is optional and which mandatory to achieve the purpose,**<br>2) the **means used for Collection, Processing, storage and Destruction** of Personal Data. | Provides broader scope of situations, where Privacy Impact Assessment is needed.<br><br>It is necessary where there is **processing of Sensitive Data** or **collecting, comparing, or linking two or more sets of Personal Data obtained from different sources** takes place. | | Consent does not create a basis for the transfer. |

# Legal Bases

| | | Consent | Contract compliance | Legal obligation | Interest of DS | Public-related bases | Legitimate Interest of DC |
|---|---|---|---|---|---|---|---|
| Major similarities: GDPR v. PDPL | | 1) Freely **given, specific, informed and unambiguous**<br>**2) Explicit for sensitive data** or **in case of automated individual decision-making**<br>3) Withdrawal at **any time** | One of the parties to the contract must be the data subject | / | / | / | 1) Processing must be **necessary**<br>2) Basis **cannot be used to process Sensitive Data**<br>3) Processing must be without prejudice to the rights and interests of the data subject |
| Major differences | PDPL | 1) Explicit also for processing of **Credit Data** | 1) Processing must "implement" a contract<br>2) Processing must be done after concluding a contract (i.e., "*in implementation of a previous agreement*"). | Processing is done "*pursuant to another law*" | 1) Processing serves "Actual" interest of the data subject – **broader scope than GDPR**<br>2) But only if communicating with the data subject is impossible or difficult | 1) No "public interest" purpose<br>2) Processing done only by a (1) **Public Entity** for (2) **security purposes or** (3) **to satisfy judicial decisions** | **1) Does not cover interest of a third party** – it must be the interest of the controller<br>2) Cannot be used for direct marketing (consent is the only basis to be used for direct marketing) |
| | GDPR | **1) Consent should be also explicit if** it is **a basis for a data transfer outside EEA** | 1) Processing is **necessary for the performance** of a contract and/or<br>2) Processing is carried out at the request of the data prior to entering into a contract; | Processing must be "*necessary for compliance with legal obligation*" | Processing serves "Vital" interest of the data subject (for e.g., protecting the data subjects' life). | Processing must be **(1) necessary** to carry out a task in the public interest or **(2)** in the **exercise of official authority** vested in the controller | 1) Covers explicitly not only interest of the controller but also of a third party<br>2) Allowed to be used for direct marketing |

# Data Subject Rights

| | | Right to Be Informed | Access | Rectification | Portability | Erasure/Destruction | Objection | Restriction | Complain | Withdrawal |
|---|---|---|---|---|---|---|---|---|---|---|
| Applicability | GDPR | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | PDPL | ✓ | ✓ | ✓ | ✓ | ✓ | ? | ✓ * | ✓ | ✓ |
| Comments re. PDPL | | Like GDPR, scope is broader if the source of data is not the data subject directly – the controller must inform about the source and categories of data processed. | | | A right to export data. The part about transmitting data to another controller is skipped. Data subjects may request hard copies if feasible. No "basis" limitations as under GDPR. | | There is no explicit / direct right to object data processing. | *Not explicitly referred to as a separate right under PDPL – applicable, where data is incomplete or inaccurate. | Similar to GDPR. | The controller must implement measures to make consent withdrawal possible.<br><br>Withdrawing consent should be similar to or easier than obtaining one. |

For any further inquiries or to explore our services in detail, please reach out to us at:

hello@whitellabelconsultancy.com

Or on our website:

www.whitelabelconsultancy.com

White Label Consultancy