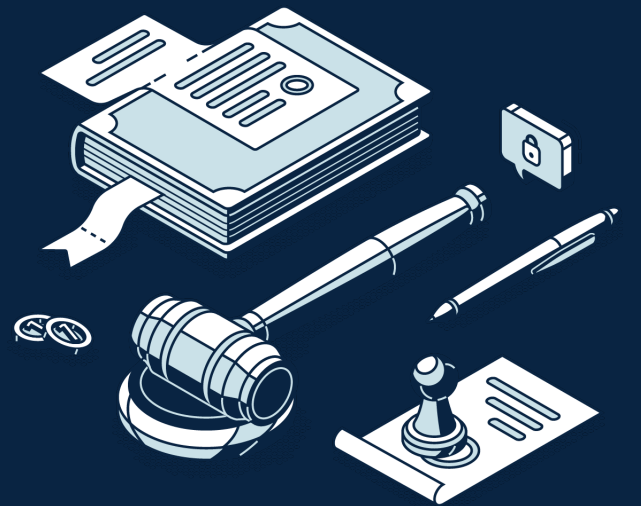
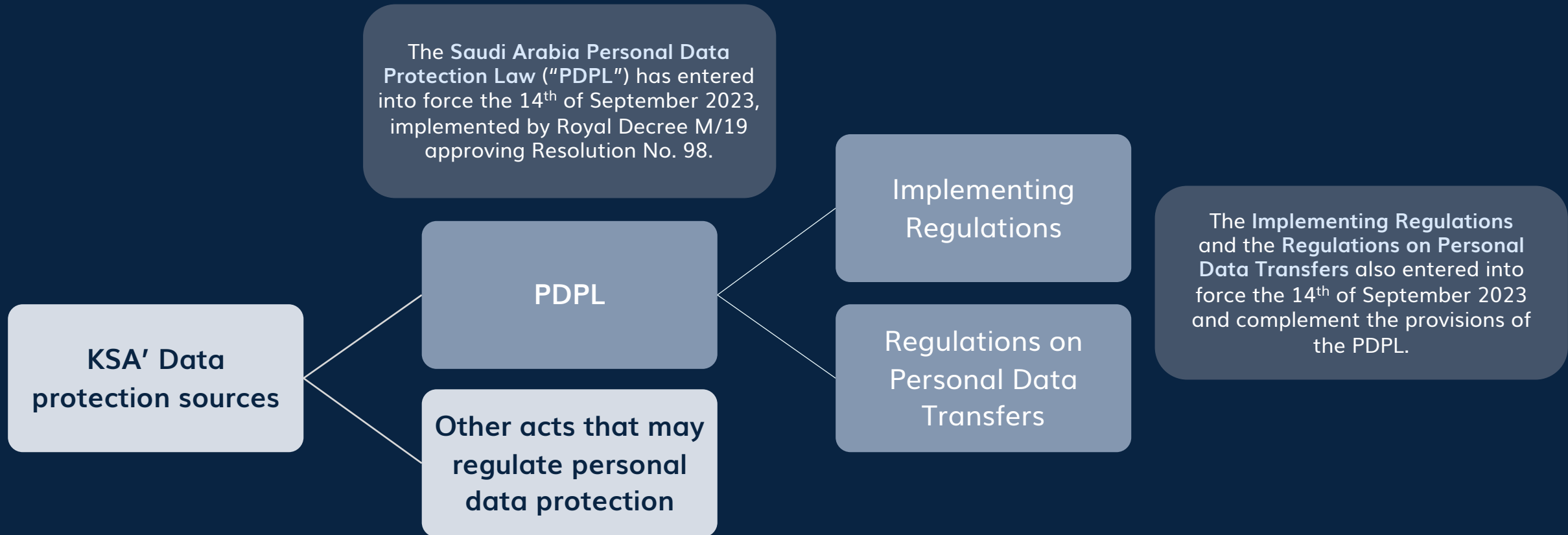


KSA takes on personal data protection

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	<p>Similarly understood definitions of Data, Processing, Processor, Controller, Transfer, Data Subject.</p> <p>Uses the same concepts as RoPA, DPO, family use exception.</p>	<ol style="list-style-type: none"> 1) 72 hours to notify DPA about a breach 2) The controller must provide DPA with details of the breach (e.g., description, risks identified, actions / measures taken); 3) The controller must notify the data subjects without undue delay if certain conditions are met. 	<p>Should specify:</p> <ul style="list-style-type: none"> • Legal basis • Purpose of collection and • Information about the Data Subject rights and how to exercise them • Recipients • Consequences of not providing the data by the data subject 	<p>Should be carried out if certain conditions are met.</p> <p>Both mandate to do an Assessment if the processing re. processing data on large scale or monitoring data subjects</p>	<p>Provide certain conditions which – if satisfied – oblige controllers to appoint a DPO.</p>	<p>Similar transfer mechanisms as: adequacy decisions; standard contract clauses; BCRs.</p> <p>Transfer Impact Assessment as a required component of the process.</p>
Major differences under PDPL	<p>PDPL also introduces some specific definitions, such as:</p> <ol style="list-style-type: none"> 1) Credit Data 2) Health Data 3) Health Services 4) Publishing. 		<ol style="list-style-type: none"> 1) Also, it should specify Personal Data to be collected, which data is optional and which mandatory to achieve the purpose, 2) the means used for Collection, Processing, storage and Destruction of Personal Data. 	<p>Provides broader scope of situations, where Privacy Impact Assessment is needed.</p> <p>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.</p>		<p>Consent does not create a basis for the transfer.</p>

Legal Bases

		Consent	Contract compliance	Legal obligation	Interest of DS	Public-related bases	Legitimate Interest of DC
Major similarities: GDPR v. PDPL		<ol style="list-style-type: none"> 1) Freely given, specific, informed and unambiguous 2) Explicit for sensitive data or in case of automated individual decision-making 3) Withdrawal at any time 	One of the parties to the contract must be the data subject	/	/	/	<ol style="list-style-type: none"> 1) Processing must be necessary 2) Basis cannot be used to process Sensitive Data 3) Processing must be without prejudice to the rights and interests of the data subject
Major differences	PDPL	<ol style="list-style-type: none"> 1) Explicit also for processing of Credit Data 	<ol style="list-style-type: none"> 1) Processing must "implement" a contract 2) Processing must be done after concluding a contract (i.e., "in implementation of a previous agreement"). 	Processing is done " <i>pursuant to another law</i> "	<ol style="list-style-type: none"> 1) Processing serves "Actual" interest of the data subject – broader scope than GDPR 2) But only if communicating with the data subject is impossible or difficult 	<ol style="list-style-type: none"> 1) No "public interest" purpose 2) Processing done only by a (1) Public Entity for (2) security purposes or (3) to satisfy judicial decisions 	<ol style="list-style-type: none"> 1) Does not cover interest of a third party – it must be the interest of the controller 2) Cannot be used for direct marketing (consent is the only basis to be used for direct marketing)
	GDPR	<ol style="list-style-type: none"> 1) Consent should be also explicit if it is a basis for a data transfer outside EEA 	<ol style="list-style-type: none"> 1) Processing is necessary for the performance of a contract and/or 2) Processing is carried out at the request of the data prior to entering into a contract; 	Processing must be " <i>necessary for compliance with legal obligation</i> "	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	<ol style="list-style-type: none"> 1) Covers explicitly not only interest of the controller but also of a third party 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. 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@whitelabelconsultancy.com

Or on our website:

www.whitelabelconsultancy.com

