Kingdom of Saudi Arabia Personal Data Protection Law Series

Part 2 - Summary of the Implementing Regulation

pwc

Introduction

From 14 September 2024 the Implementing Regulation will become enforceable in the Kingdom of Saudi Arabia ("**KSA**"). The Implementing Regulation provides further details to the existing requirements of the Personal Data Protection Law ("**PDPL**").

In this part 2 of PDPL Series we provide overview of some of the key requirements of the Implementing Regulation to the PDPL. Please refer to part 1 of PDPL series for overview of the PDPL and its key concepts.

Key requirements of the Implementing Regulation

Governance

- The Implementing Regulation requires the Controller to appoint a Data Protection Officer ("**DPO**") in any of the following cases:
  - the Controller is a public entity that provides services involving processing of personal data on a large scale;
  - primary activities of the Controller consist of processing operations that require regular and continuous monitoring of individuals; or
  - core activities of the Controller consist of processing sensitive personal data.

- The Implementing Regulation specifies key responsibilities of the DPO as follows:
  - to act as the direct point of contact with the Competent Authority (SDAIA) and implement its decisions and instructions;
  - to supervise the impact assessments that need to be undertaken, audit reports, and evaluations, document the assessment results;
  - monitor and update the records of personal data processing activities ("**RoPA**");
  - enable the data subjects to exercise their rights;
  - respond to data subjects' requests and address their complaints;
  - notify the Competent Authority and data subjects of data breaches as applicable; and
  - handle the Controller's violations related to personal data and take corrective actions accordingly.

According to Art. 32 (4) of the Implementing Regulation, the Competent Authority will issue rules for the appointment of a DPO, the circumstances under which a DPO should be appointed, as well as their duties and responsibilities.

Art. 32

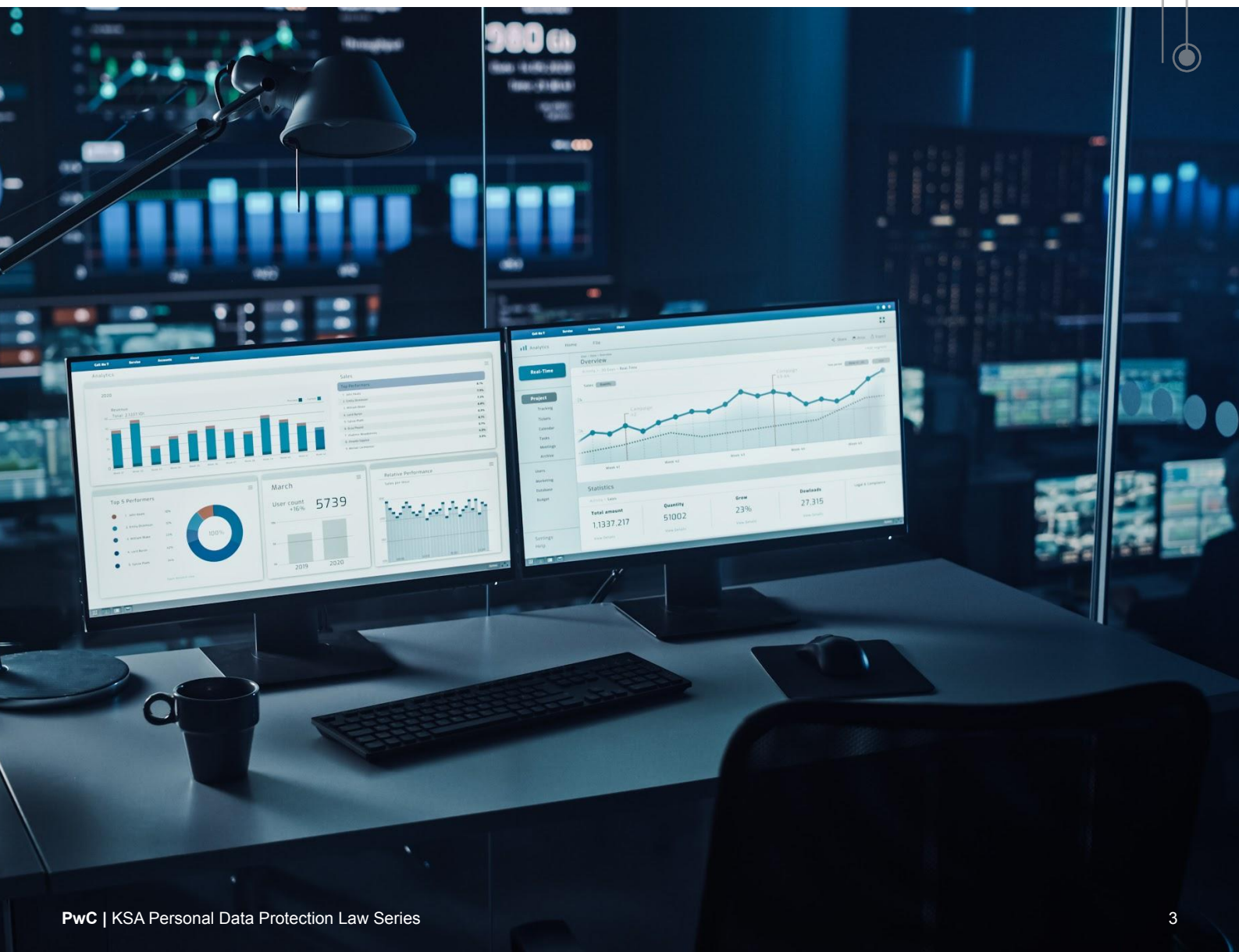
Data subject rights

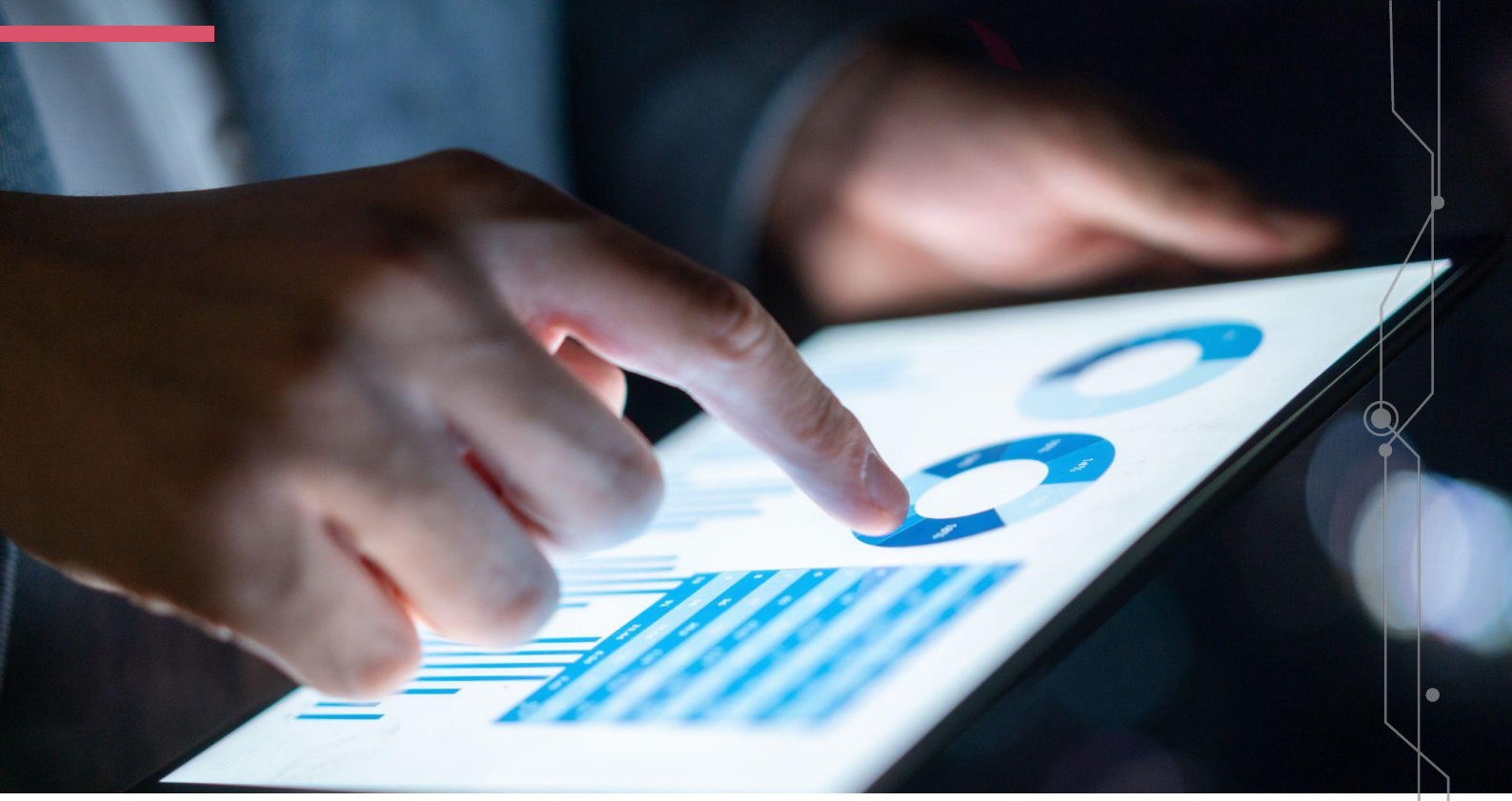
The Implementing Regulation sets out the rules that the Controller shall follow upon receiving a request from a data subject. For instance, the Controller must:

- comply with the request within a period not exceeding 30 days, which can be extended up to an additional 30 days in case the response requires disproportionate effort, or if the Controller receives multiple requests from the data subject;
- take the necessary technical, administrative, and organisational measures to ensure a prompt response to requests;
- take appropriate measures to verify the identity of the requester before executing the request; and
- take the necessary measures to document and keep record of all submitted requests, including verbal requests.

The Controller may refuse to act on the request when it is repetitive, manifestly unfounded, or requires disproportionate efforts.

Art. 3





The Implementing Regulation provides for additional details on how the Controller shall ensure that the data subjects can exercise their rights, in particular:

- the right to be informed (including what information shall be provided to the data subject and how);
- the right of access to the data (including the safeguards aiming at protecting personal data when it is disclosed);
- the right to rectification (including the right of the data subject to request restriction of processing of personal data while the accuracy of personal data is contested, etc.); and
- the right to destruction of the data (including when and how such destruction can be performed).

Art. 4 - 8

The Regulation provides for details on how a data subject can make a complaint to the Competent Authority, for instance:

- the timelines within which a complaint can be made (in particular, it cannot exceed 90 days from the date of the incident or the date on which the data subject became aware of it);
- the contents of the complaint; and
- key actions that the Competent Authority shall take in relation to the complaint.

Art. 37

Consent

- The Implementing Regulation specifies requirements to the consent as the lawful basis for processing of personal data:
  - consent shall be given freely and not obtained through misleading methods;
  - processing purposes shall be clear, specific, and shall be explained and clarified to the data subject before or at the time of requesting consent;
  - consent shall be given by a person who has full legal capacity;
  - consent shall be documented;
  - independent consent shall be obtained for each processing purpose;
  - before requesting consent from the data subject, the Controller shall establish procedures that allow for the withdrawal of that consent; and
  - in the event of withdrawal of consent, the Controller shall cease processing without undue delay after the withdrawal request.
- The Implementing Regulation specifies that in some cases the consent must be explicit, in particular when:
  - the processing involves sensitive data; or
  - the processing involves credit data; or
  - decisions are made solely based on automated processing of personal data.

Explicit consent means 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 intention can be proven. In essence, there must be a positive action for the data subject to take to acknowledge the consent (for example: clicking an unticked consent box).

Art. 11-12

Legitimate interest

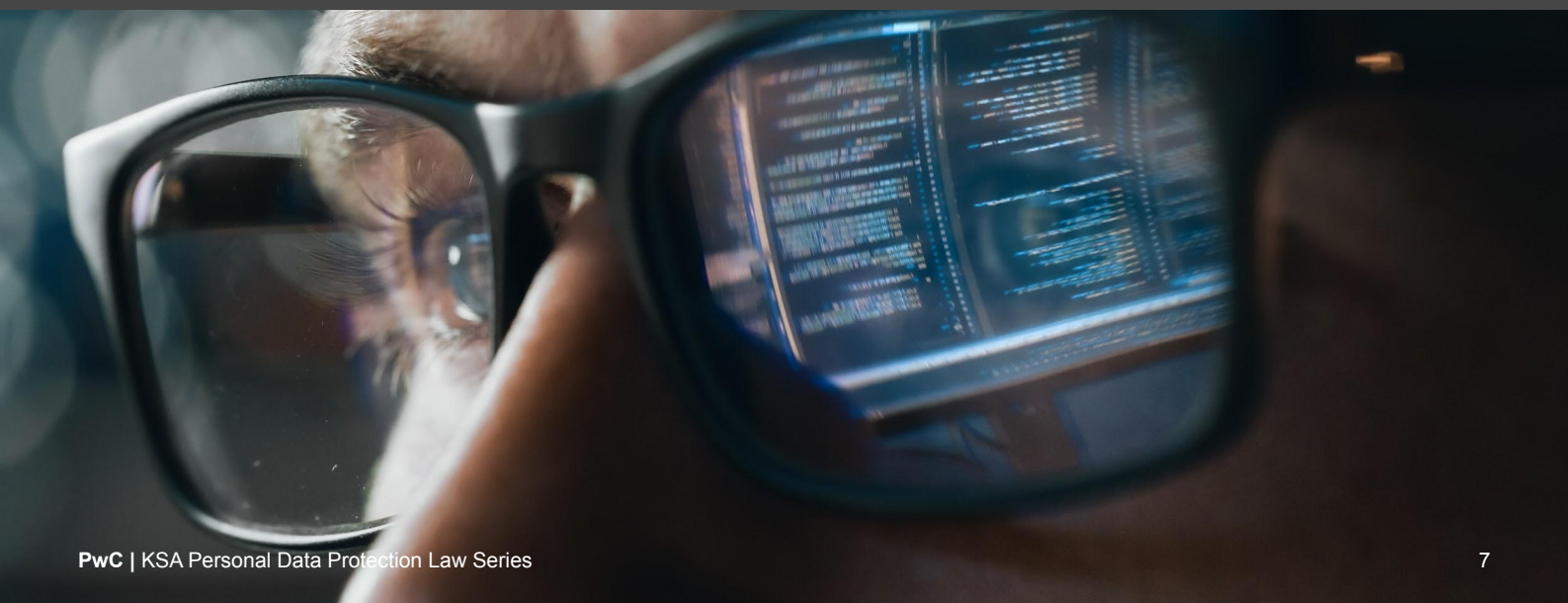
- The Implementing Regulation specifies requirements for using legitimate interest as a lawful basis. For instance, legitimate interest can be used if the following conditions are met:
  - purpose of processing shall not violate any of the laws in the KSA;
  - there is a balance between the rights and interests of the data subject and the legitimate interest of the Controller, so that the interests of the Controller do not affect the rights and interests of the data subject;
  - processing shall not include sensitive data; and
  - processing shall be within the reasonable expectations of the data subject.
- Before processing personal data for legitimate interests, the Controller shall conduct and document an assessment of the proposed processing and its impact on the rights and interests of data subjects which must include:
  - identification of the proposed processing and its purposes, as well as the type of data and categories of data subjects;
  - evaluation of the purpose to ensure that it is legitimate and compliant with the laws in the KSA;
  - verification of the necessity to process personal data to achieve the legitimate purpose of the Controller;
  - evaluation of whether the proposed processing will cause any potential harm to data subjects or their ability to exercise their rights; and
  - identification of any measures to be taken to avoid potential risks or harm.

Art. 16

Risk management

- The Implementing Regulation specifies the cases when the Controller must conduct data protection impact assessments ("**DPIA**"). In particular when:
  - the processing involves the processing of sensitive data;
  - the Controller collects, compares, or links two or more sets of personal data obtained from different sources;
  - the activity of the Controller includes continuous and large scale processing of personal data of those who fully or partially lack legal capacity, or processing operations that by nature require continuous monitoring of data subjects, or processing personal data using new technologies, or making decisions based on automated processing of personal data; or
  - the Controller provides a product or service that involves processing personal data that is likely to cause serious harm to the privacy of data subjects.
- The Implementing Regulation specifies requirements to the content of the DPIA which should include the following information (to be specified in the DPIA report):
  - the purpose of the processing and its lawful basis;
  - a description of the nature of processing, types, sources of personal data, entities to which the personal data is disclosed;
  - a description of the scope of processing;
  - a description of the context of processing;
  - an assessment of necessity and proportionality of the measures to be taken;
  - the impact of processing based on the severity of its impact, materially and morally, and the likelihood of any negative impact on data subjects;
  - the measures that will be taken to prevent or limit the risks; and
  - an evaluation of the suitability of the measures envisaged to avoid identified risks.

Art. 25



Data lifecycle management

The Implementing Regulation specifies requirements for maintenance of the records of processing activities ("**RoPA**"). The RoPA shall include the following information:

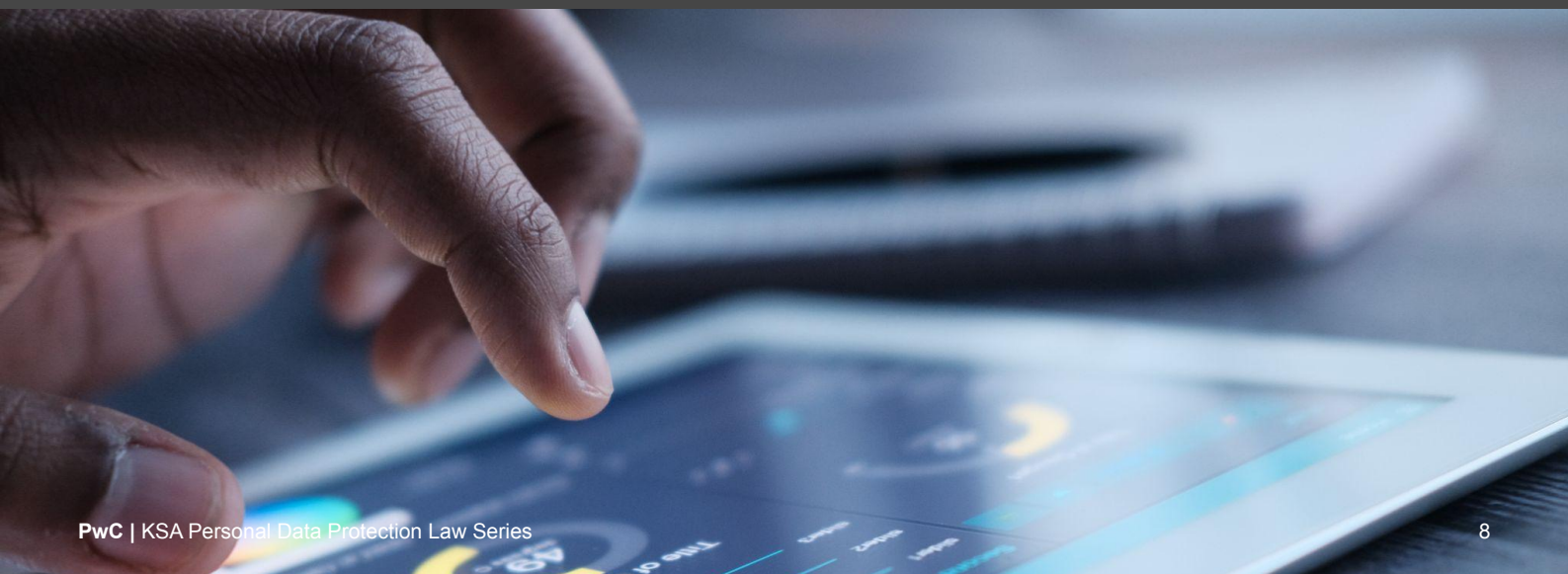
- Controller's name and relevant contact details;
- information about the DPO, if the DPO is required in accordance with Art. 32 of the Implementing Regulation;
- purposes of personal data processing;
- description of the categories of personal data being processed;
- the categories of data subjects;
- retention periods for each category of personal data;
- categories of recipients to whom the personal data is disclosed;
- description of personal data transfers outside the KSA, including the lawful basis for the transfers and the recipients of the personal data;
- description of the procedures and the organisational, administrative, and technical measures in place that ensure the security of personal data.

Art. 33

The Implementing Regulation provides for requirements to certain types of personal data processing activities, for instance:

- processing of health data;
- processing of credit data;
- processing data for advertising or awareness purposes;
- processing data for direct marketing;
- processing data for scientific, research or statistical purposes.

Art. 26-30

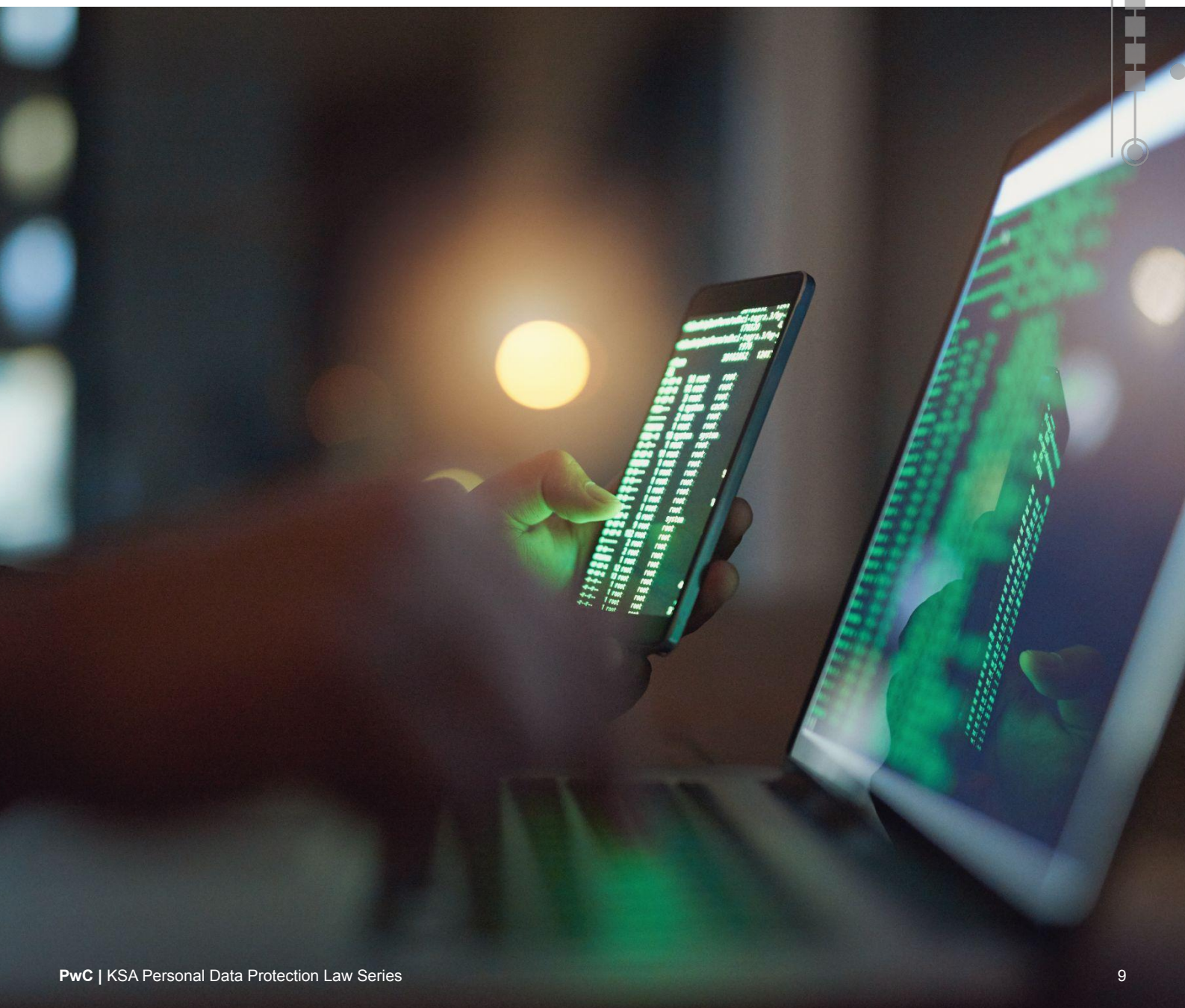


Data breach management

The Implementing Regulation provides for details on the obligation of the controller to notify the Competent Authority and data subjects of a personal data breach:

- The Controller shall make notification to the Competent Authority within 72 hours of becoming aware of the incident, if such incident potentially causes harm to the personal data, or to data subject or conflict with their rights or interests.
- The Controller shall, without delay, make notification to data subjects if the breach may cause damage to their data or conflict with their rights or interests.
- The Implementing Regulation specifies requirements to the content of the breach notification to be made to the Competent Authority or data subjects.

Art. 24



Third-party management

The Implementing Regulation specifies key requirements to cooperation between the Controller and the Processor. In particular:

- the terms and conditions to be included in the data processing agreement between the Controller and the Processor must include, at a minimum, the following:
  - the purpose of processing;
  - categories of personal data being processed;
  - the duration of the processing;
  - the Processor's obligation to notify the Controller of a personal data breach;
  - information on whether the Processor is subject to regulations in other countries and the impact on their compliance with the Law and its Regulations;
  - obligation of the Processor to notify the Controller of the disclosure of personal data which could be mandatory under the applicable laws of the KSA;
  - identifying any subcontractors contracted by the Processor, or any other party to whom personal data will be disclosed.
- the Controller shall issue clear instructions to the Processor;
- the Controller shall assess Processor's compliance with the PDPL and Regulations; and
- the Processor shall comply with certain requirements when entering into agreements with sub-processors.

Art. 17

Data security

The Implementing Regulation provides for details on the measures to be taken by the Controller to ensure the security of personal data. For instance, the Implementing Regulation requires the Controller:

- to implement necessary security and technical measures to limit security risks related to personal data breach;
- to comply with relevant controls, standards, and rules issued by the KSA National Cybersecurity Authority or recognised best practices and cybersecurity standards if the Controller is not obligated to follow the controls, standards, and rules issued by the KSA National Cybersecurity Authority.

Art. 23

Get in Touch

To discuss how PwC can support you with implementing your data privacy programme, please get in touch.

Phil Mennie
Partner, Cybersecurity and Digital Trust
+971 56 369 7736
phil.mennie@pwc.com
linkedin.com/in/philmennie @philmennie

Richard Chudzynski
PwC Data Privacy Legal Leader
+971 56 417 6591
richard.chudzynski@pwc.com
linkedin.com/in/richardchudzynski

Thank you

About PwC

Established in the Middle East for 40 years, PwC has 22 offices across 12 countries. As a community of solvers, with 8,000 people across the region, we bring the right combination of people, technology and expert capabilities from Strategy, through Advisory and Consulting to Tax and Assurance Services, to solve the region's most pressing challenges (www.pwc.com/me).