Kingdom of Saudi Arabia Personal Data Protection Law Series

Part 3 - Summary of the Data Transfer Regulations

pwc

Summary of the Data Transfer Regulation

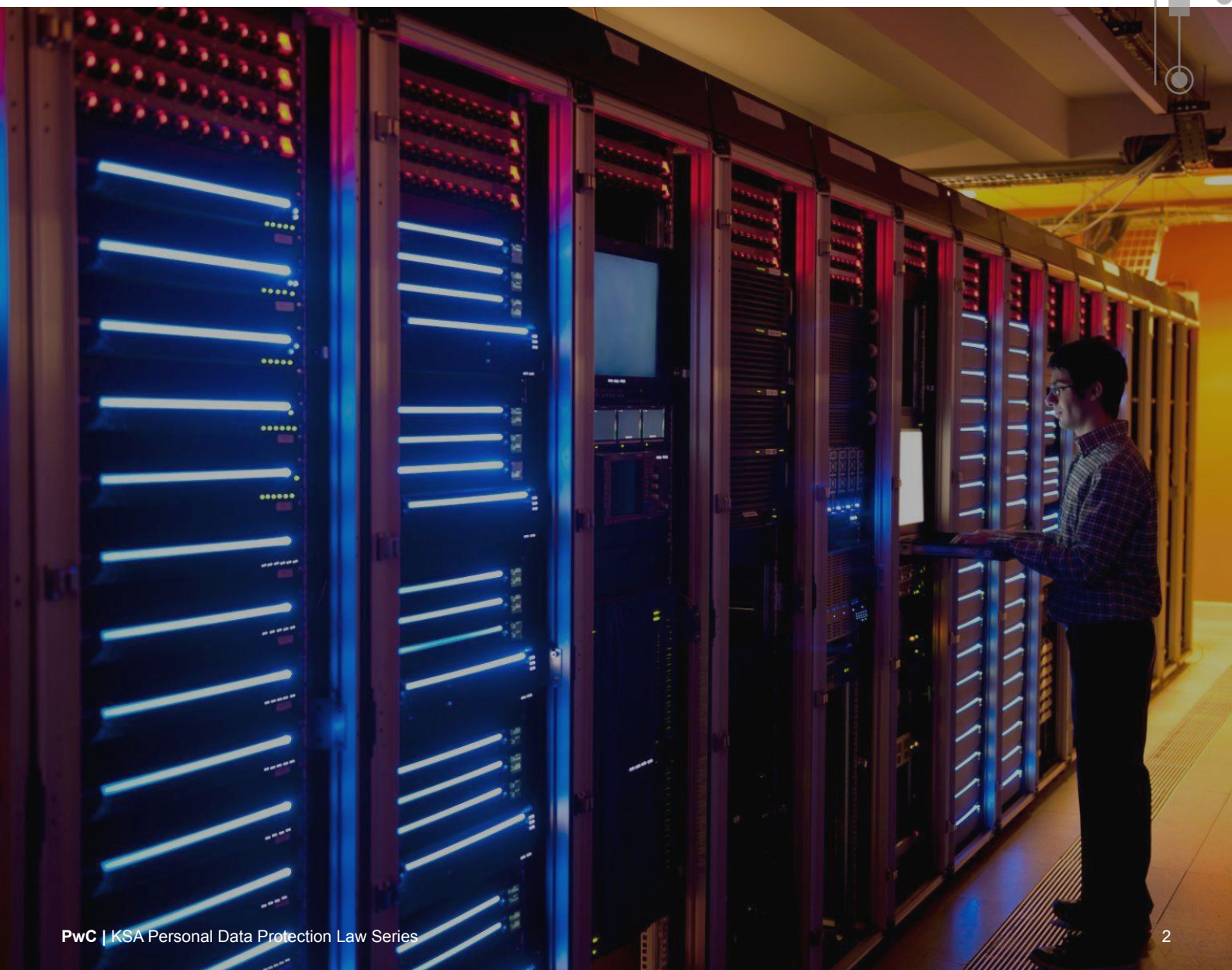
Introduction

On 7 September 2023, the Regulation on Personal Data Transfer outside the Kingdom (Data Transfer Regulation) was published in the Kingdom of Saudi Arabia (KSA). The Data Transfer Regulation provides details to the existing requirements of Article 29 of the Personal Data Protection Law ("Law") on cross-border personal data transfers. The Data Transfer Regulation will come into force on 14 September 2024. From this date the Law will also become fully enforceable.

The Data Transfer Regulation is essential in helping entities to address various concerns related to the movement of personal data across borders. It serves as a framework to ensure the secure and responsible cross-border personal data flows.

In this Part 3 of our "Kingdom of Saudi Arabia Personal Data Protection Law Series", we provide a **step-by-step guide on the rules on cross-border personal data transfers**.

Our guide is based on the current text of the Law and the Data Transfer Regulations. It is expected that the Saudi Data & AI Authority ("SDAIA") will issue a separate guidance document on the topic in due course.



Terms and definitions

Transfer of personal data[1] is the transfer of personal data outside the geographical boundaries of KSA for the purpose of processing.

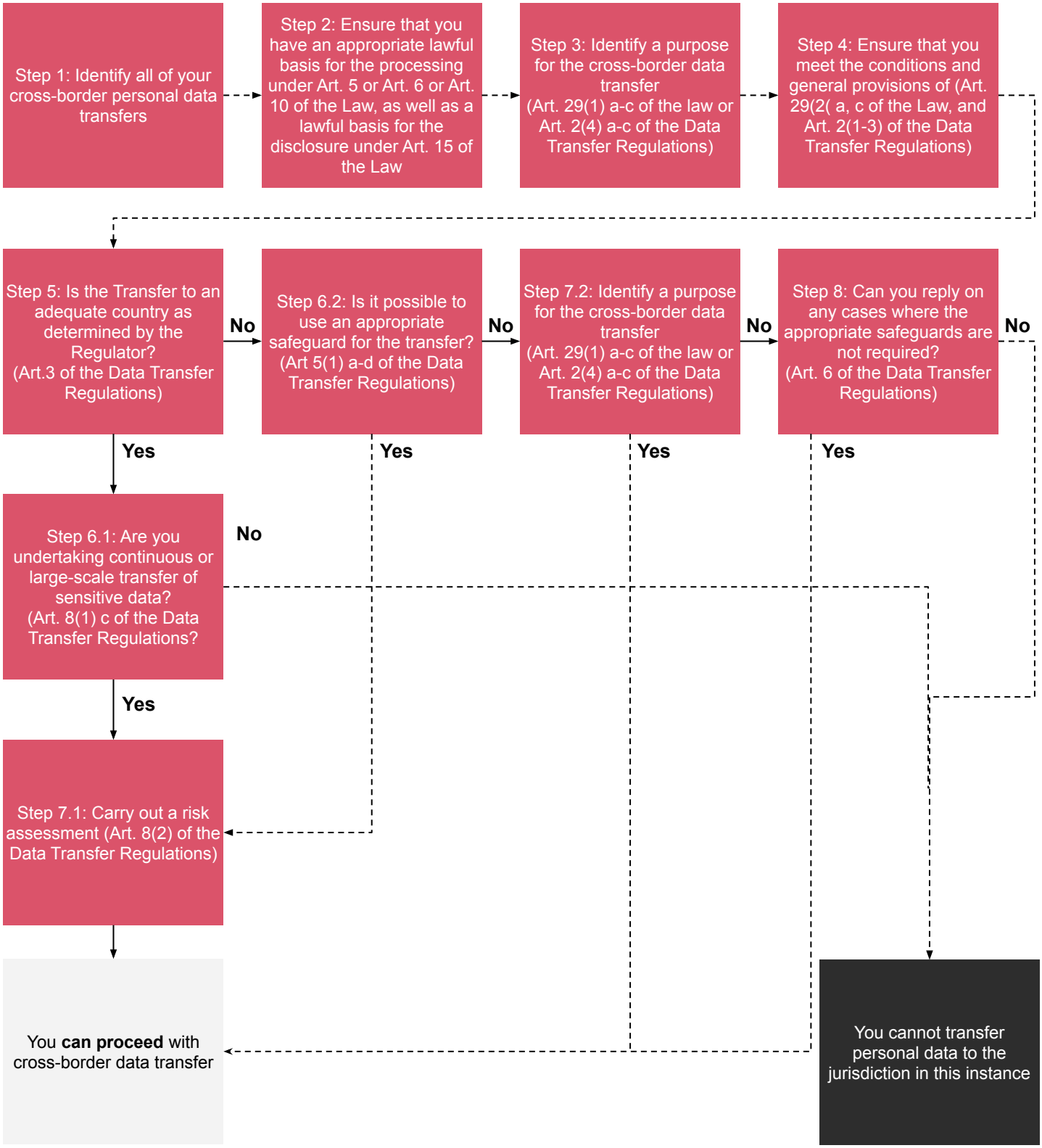
Disclosure is enabling any person - other than the controller or the processor, as the case may be - to access, collect or use personal data by any means and for any purpose.

Controller is an entity that determines the purpose and manner of processing personal data, whether the data is processed by that controller or by the processor.

Processor is any entity that processes personal data for the benefit and on behalf of the controller.

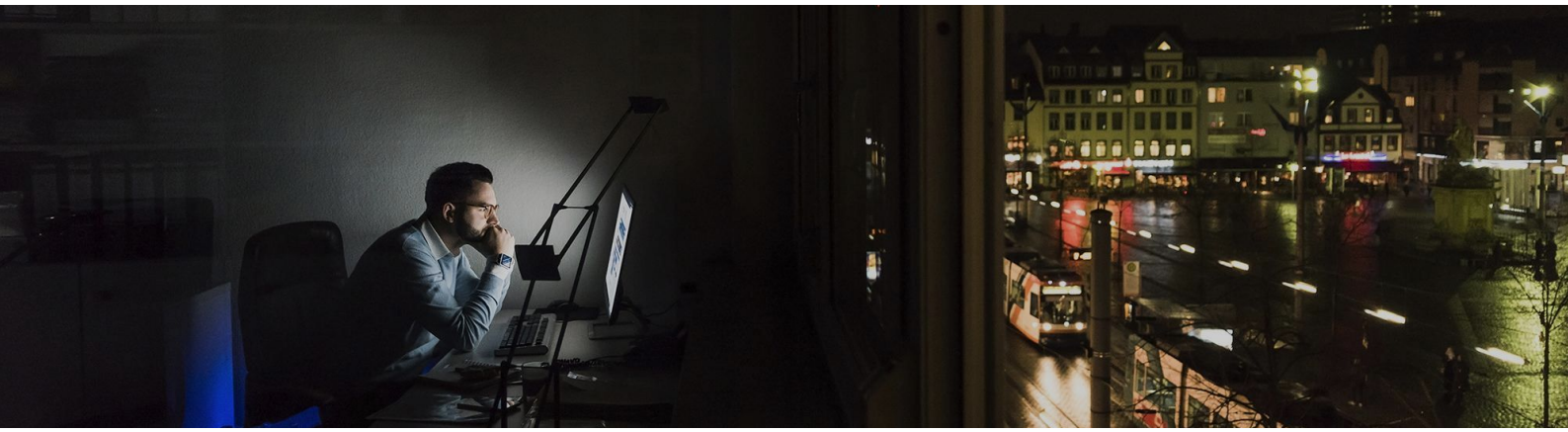
[1] In this series we use the terms “transfers of personal data” and “cross-border personal data transfer” interchangeably.

Steps for lawful cross-border personal data transfers



Below we have outlined the steps which, if carried out correctly, will allow a lawful transfer of personal data. It is important that these steps are carried out in the sequence, as outlined below.

Step	Description of the step	Article
Step 1	The controller must first identify its existing and planned personal data processing activities involving cross-border personal data transfers. Such activities must be recorded in the internal document of the controller - the records of processing activities, after this the controller may proceed to **Step 2**.	**Art. 31 of the Law**
Step 2	The controller must ensure that it has an appropriate **lawful basis for the processing** (as per Art. 5 or 6 or 10 of the Law), as well as a **lawful basis for the disclosure** of the personal data (as per Art. 15 of the Law)[2]. For an overview of these lawful bases please see the link to Part 1 of the PDPL series. After ensuring that the appropriate lawful bases are in place (for processing and disclosure), the controller may proceed to **Step 3**.	**Art. 5, 6 or 10 and 15 of the Law**



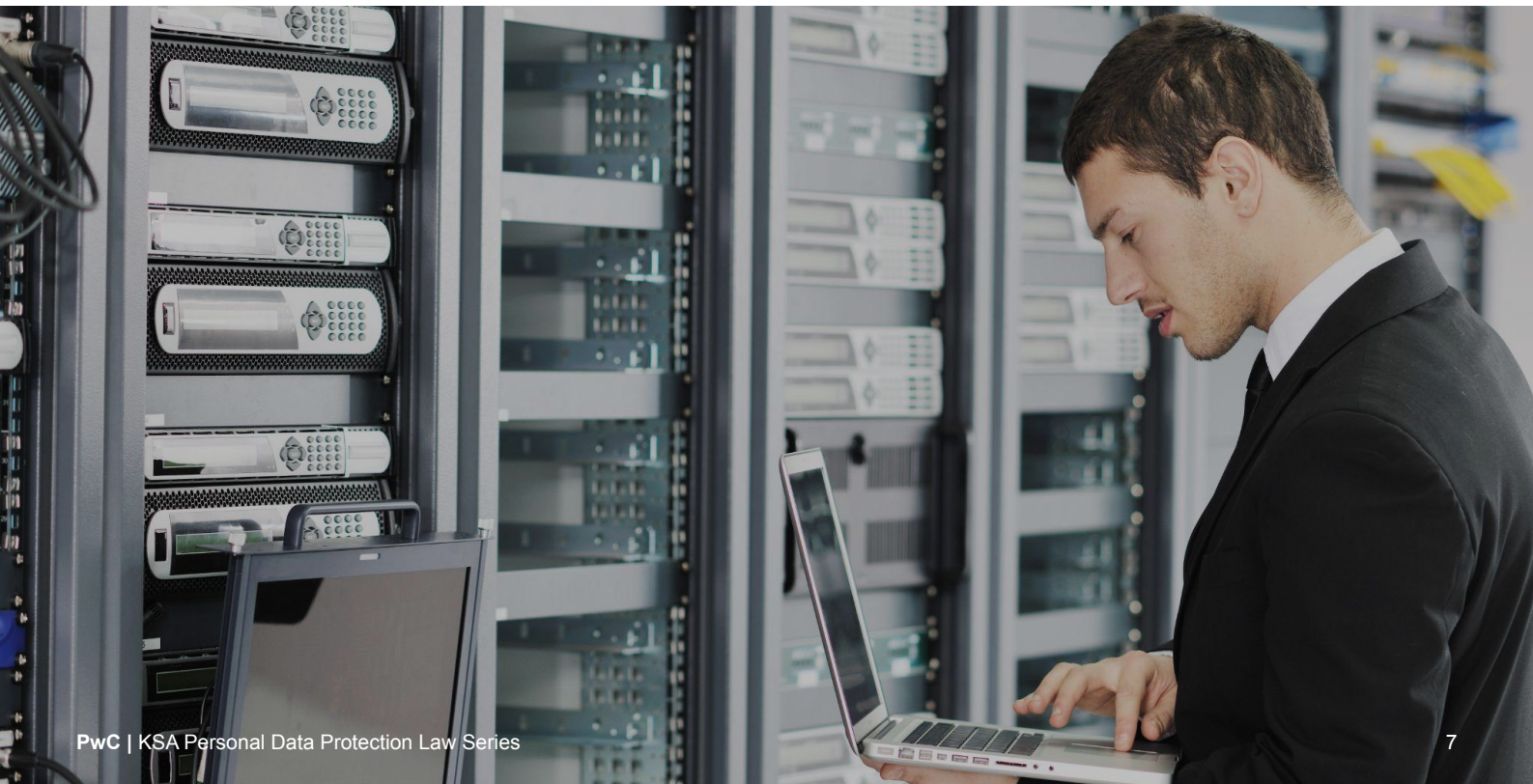
[2] Please note that in general cross-border personal data transfer will be considered as a disclosure under Art. 15 of the Law (e.g. transfer of personal data from one legal entity to another legal entity - including within the same group). The controller will need to ensure that:

1. it has in place a legal basis for disclosure from those bases specified in Art. 15 of the Law (this requirement of having a lawful basis is in addition to that under Art 5 or 6 or 10 of the Law);
2. ensure that the disclosure is a permitted disclosure. The controller may not disclose personal data in the cases set out in Article 16 of the Law; and
3. if it is a permitted disclosure - ensure that sufficient guarantees are in place as applicable if the disclosure is to a processor in accordance with Art 17 of the Implementing Regulation to the Law.

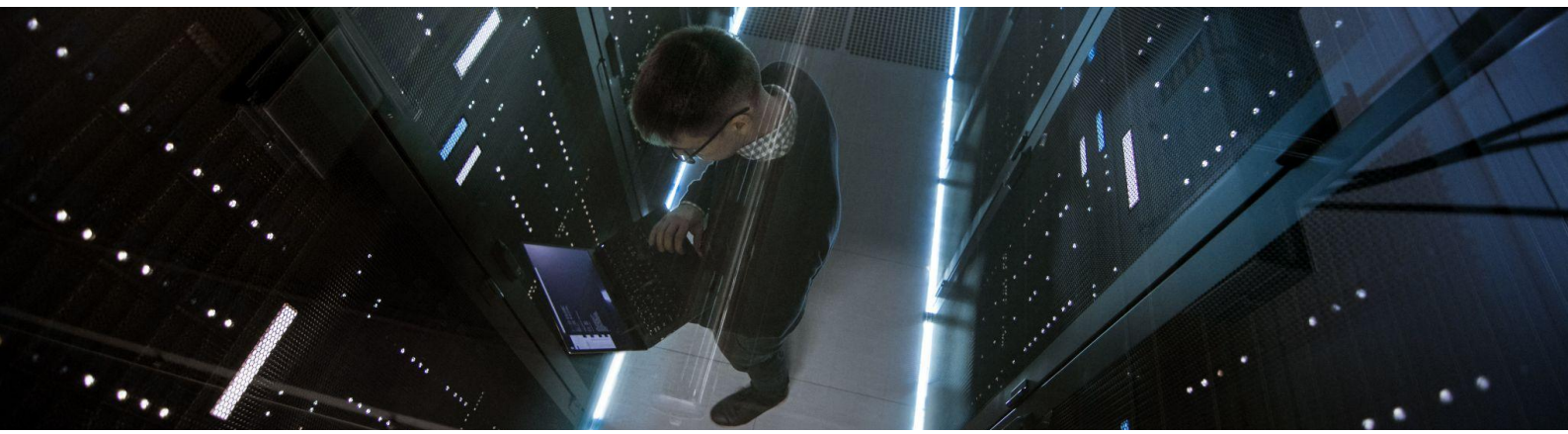
Step	Description of the step	Article
Step 3	The controller must assess if it can use one of the following purposes for cross-border personal data transfer. **Compliance with international agreements** to which KSA is a party (e.g., trade, security, or diplomatic agreements). **National interests** of the KSA (e.g., national security, economic development, or other strategic goals). **Data subject's obligations under agreements or contracts**, to which the data subject is a party. **Controller's operational activities** (e.g., various business operations, including central management operations, administrative functions, and other processes that are important for the controller's functions). **Data subject's benefits** (e.g., services or benefits might include access to various services, seamless international travel, or improved customer experiences). **Scientific research and studies**. If the controller may rely on any of the above-mentioned purposes, the controller may proceed to **Step 4**.	**Art. 29 (1) of the Law, Art. 2 (4) of the Data Transfer Regulations**
Step 4	The controller must ensure that the conditions of Art. 29 (2) (a), (c) of the Law, and the general provisions under Art. 2 (1) - (3) of the Data Transfer Regulations are met. In particular: • The transfer shall not cause any prejudice to national security or the vital interests of the Kingdom[3]. • The transfer shall be limited to the minimum amount of personal data needed[4]. • The transfer does not impact the privacy of data subjects or the level of protection guaranteed for Personal Data under the Law and its Implementing Regulations. If the controller meets all of the above-mentioned conditions, the controller may proceed to **Step 5**.	**Art. 29 (2) (a), (c), of the Law, Art. 2 (1) - (3) of the Data Transfers Regulations**

[3] Pursuant to Art. 29 (3) of the Law this requirement shall not apply to cases of extreme necessity to preserve the life or vital interests of the data subject or to prevent, examine or treat disease. However it is not quite clear if in practice any cross-border personal data transfers will be allowed if they could harm national security or the vital interests of the Kingdom. It is expected that the Saudi Data & AI Authority (SDAIA) will additionally clarify this point.
[4] Pursuant to Art. 29 (3) of the Law this requirement shall not apply to cases of extreme necessity to preserve the life or vital interests of the data subject or to prevent, examine or treat disease. However if read together with Art. 2 (2) of the Data Transfer Regulations, it may be possible to conclude that this requirement shall apply in all cases of cross-border personal data transfers, even in the above cases of extreme necessity. It is expected that the Saudi Data & AI Authority (SDAIA) will additionally clarify this point.

Step	Description of the step	Article
Step 5	The controller needs to identify whether the transfer is to a country deemed to have an **adequate level of protection**[5], as determined by the competent authority[6] in the KSA. This level of protection should not fall below the standards prescribed by the Law and the Data Transfer Regulations. The controller must proceed to **Step 6.1**, if: • it is determined by the KSA competent authority that the country, being a personal data importer, provides an adequate level of personal data protection, as determined by the KSA competent authority; or • the transfer necessary is to preserve the life or vital interests of the data subject or to prevent, examine or treat disease. • The controller must proceed to **Step 6.2**, if: • the country, being a personal data importer, is not determined by the KSA competent authority as having an adequate level of personal data protection, and at the same time • the transfer is not necessary to preserve the life or vital interests of the data subject or to prevent, examine or treat disease.	**Art. 29 (3) of the Law, Art. 3 of the Data Transfer Regulations**
Step 6.1	If the processing involves continuous or large-scale transfer of sensitive data outside the KSA the controller shall conduct a risk assessment in accordance with **Step 7**, if not – the controller can proceed with the transfer of personal data.	**Art. 8 (1) (c) of the Data Transfer Regulations**

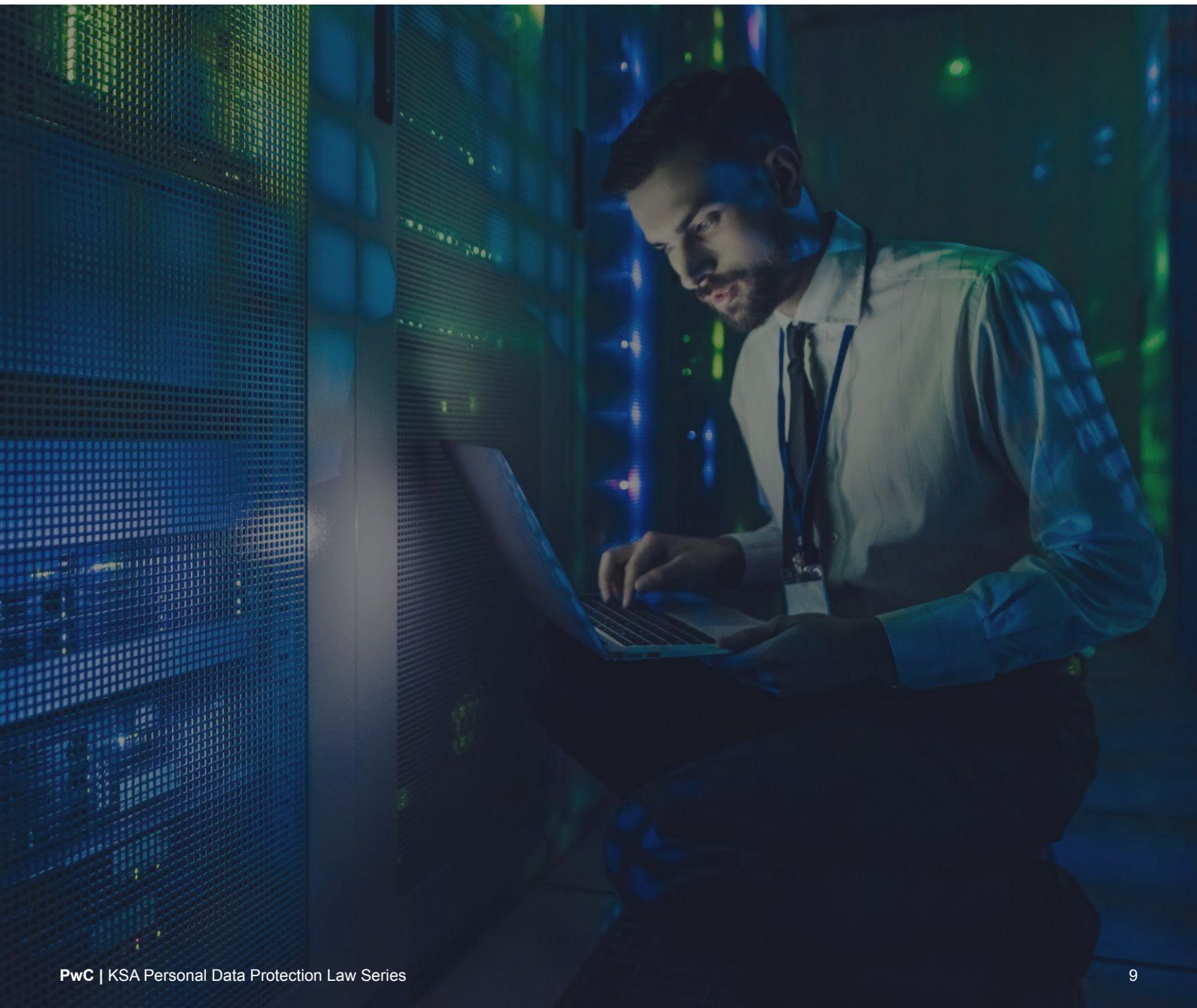


Step	Description of the step	Article
Step 6.2	The controller may transfer personal data outside the KSA, using any of the following **appropriate safeguards**[7]: **Binding Common Rules (BCR):** BCR is a framework for data protection during cross-border personal data transfers between entities engaged in a joint economic activity. BCR's must be approved by the KSA competent authority. **Standard Contractual Clauses (SCC):** SCCs shall ensure personal data protection in accordance with a standard model issued by the KSA competent authority. **Certification mechanism:** Certification of compliance with the Law and its Implementing Regulations shall be issued by an authorized entity on behalf of the competent authority, together with the enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards. **Binding Codes of Conduct:** Codes of Conduct shall be approved by the KSA competent authority, based on separate requests submitted in each case, together with the enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards. If any of the above safeguards are in place, the controller shall conduct a **risk assessment in accordance with Step 7**. In the absence of any of the above safeguards the controller must proceed to **Step 8**.	**Art. 5 (1) of the Data Transfer Regulations**



[5] As of the date of this publication the KSA authorities have not determined the countries that have adequate level of protection of personal data.
[6] As of the date of this publication the competent authority in KSA in the area of personal data is the Saudi Data & AI Authority (SDAIA).
[7] As of the date of this publication none of these safeguards have yet been implemented in the KSA.

Step	Description of the step	Article
Step 7	he controller shall conduct a risk assessment of the transfer of personal data outside the KSA. Such an assessment should include at least the following elements. 1. The purpose of the transfer or disclosure and its legal basis. 2. Description of the nature of the transfer or disclosure to be carried out and its geographical scope. 3. The means and safeguards for transferring personal data outside KSA and the extent to which they are sufficient to achieve the required level of protection for personal data. 4. Measures taken to ensure that the transfer or disclosure is limited to the minimum amount of personal data necessary to achieve the purposes. 5. The material or moral impact that may result from the transfer or disclosure, and the possibility of any harm to data subjects. 6. Measures to prevent and mitigate identified risks to protect personal data. After carrying out a risk assessment the controller **may proceed with the transfer of personal data**.	**Art. 8 (2) of the Data Transfer Regulations**



Step	Description of the step	Article
Step 8	The controller may transfer personal data outside KSA in any of the **cases** set out below as long as the Controller ensures that it has reviewed whether a possible safeguard is available to it. **Performance of an agreement:** The transfer of personal data is required for the performance of an agreement to which the data subject is a party (e.g. performance of a service or sales agreement). **National security or public interest:** If the controller is a public entity, and the transfer of personal data is required for the protection of the KSA's national security or for the public interest. **Crime investigation or prosecution:** In cases where the controller is a public entity, and the transfer of personal data is required for the investigation or detection of crimes, the prosecution of their perpetrators, or the execution of penal sanctions. **Vital interests:** The transfer of personal data is required to protect the vital interests of a data subject who is unreachable.	**Art. 6 of the Data Transfers Regulations**

If the controller transfers personal data outside the KSA within Step 6.2 or 8 (as per the table above), the controller **shall immediately stop the transfer in any of the following cases** (pursuant to Art. 7 of the Data Transfers Regulations):

1. Transfer affects national security or vital interests of the KSA.
2. If the results of the risk assessment of personal data transfer outside the KSA causes high risk to the privacy of data subjects.
3. The appropriate safeguards adopted by the controller are no longer applicable.
4. The controller is unable to enforce the appropriate safeguards.

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).

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.