

Kingdom of Saudi Arabia Personal Data Protection Law Series

Part 3 - Summary of the Data Transfer Regulations (2nd edition)



Summary of the Data Transfer Regulation

Introduction

On 1 September 2024 the Saudi Data and Artificial Intelligence Authority (“**SDAIA**”) issued an updated version of the Regulation on Personal Data Transfer outside the Kingdom (“**Data Transfer Regulation**”, “**KSA**”). It elaborates on the existing requirements of Article 29 of the Saudi Personal Data Protection Law (“**Law**”) regarding cross-border personal data transfers.

The Data Transfer Regulation came into force on the day of its [publication in the Official Gazette](#) - 1 September 2024.

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**.



Key terms and definitions

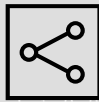
Transfer of personal data¹ is the transfer of personal data outside the geographical boundaries of KSA for the purpose of processing. This may also include access of the data stored in the KSA from abroad.



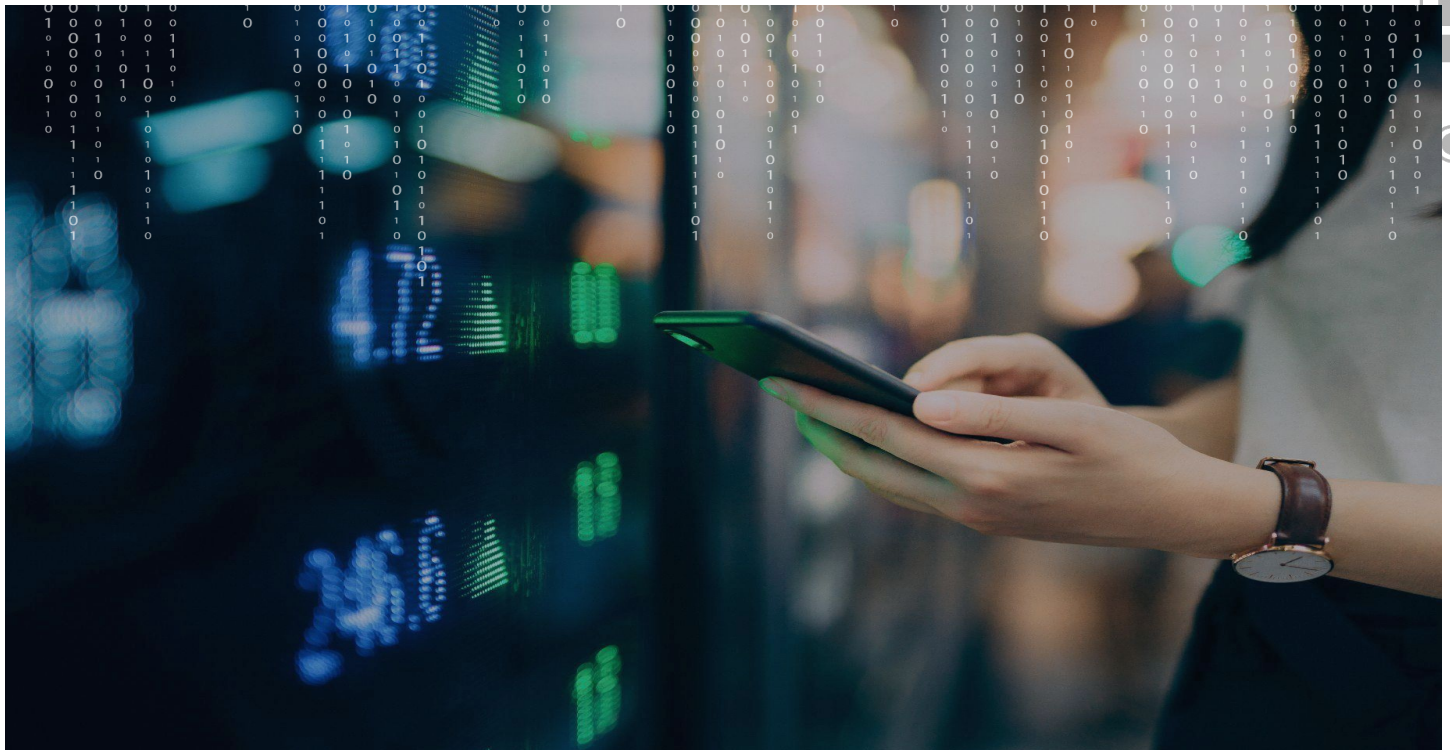
Disclosure is enabling any person - other than the controller or the processor, as the case may be - to access, collect or use personal data by any means and for any purpose.



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.

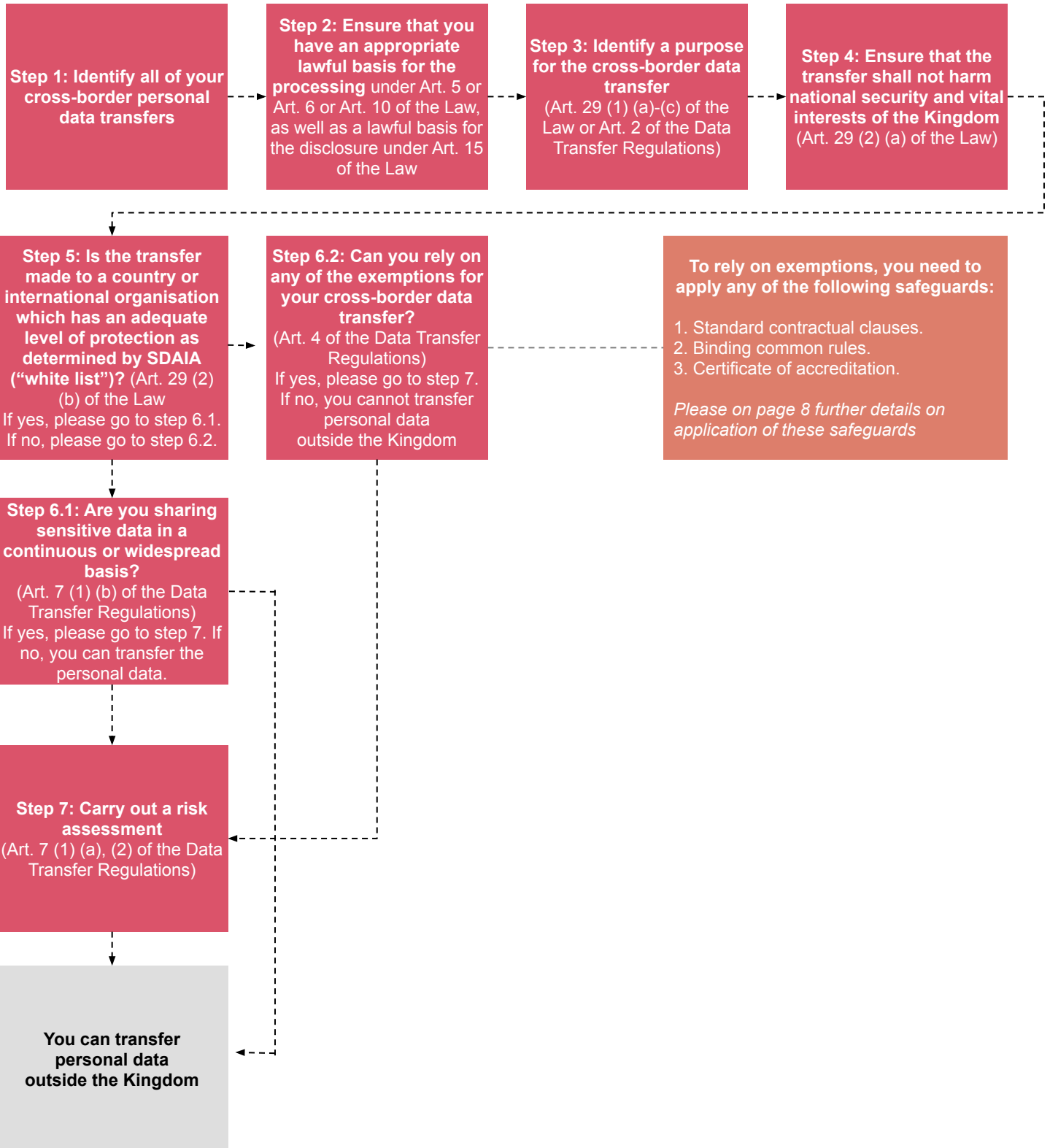


Processor is any entity that processes personal data for the benefit and on behalf of the controller.



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

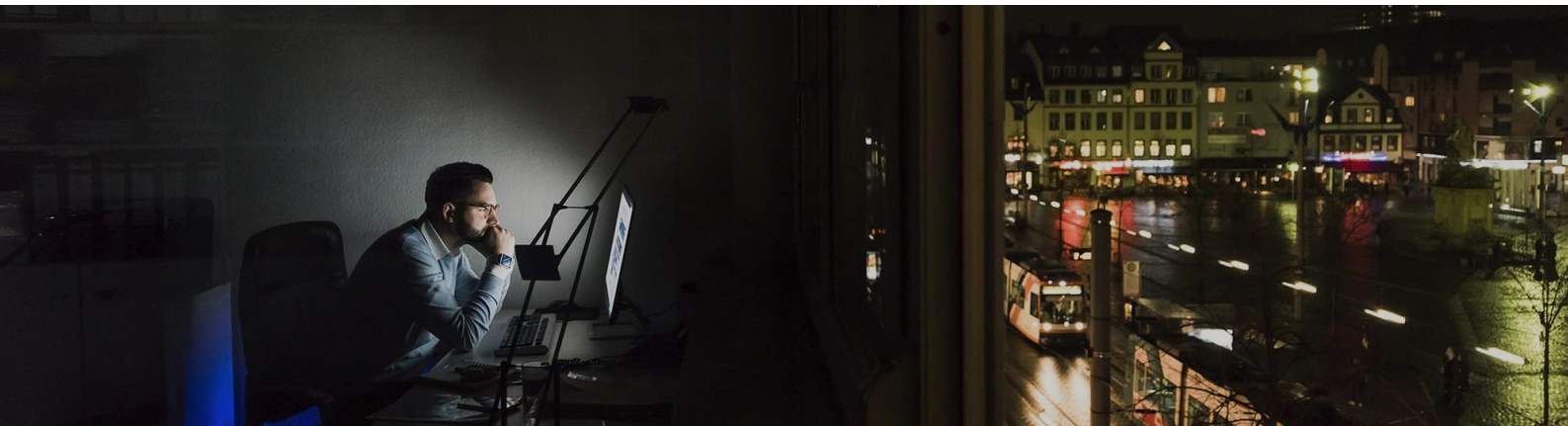
Key steps for lawful cross-border personal data transfers



Please see comments on each step on further pages.







Below we have outlined the steps which, if carried out correctly, will allow a lawful transfer of personal data outside of the Kingdom. It is important that these steps are carried out in the sequence, as outlined below. Please note that this procedure shall apply to all subsequent transfers of personal data that has been transferred or disclosed to a party outside the Kingdom.

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	<p>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.</p> <p>For an overview of these lawful bases please see Part 1 of the PDPL series.</p> <p>After ensuring that the appropriate lawful bases are in place (for processing and disclosure), the controller may proceed to Step 3.</p>	Art. 5, 6, 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 made to a processor in accordance with Art 17 of the Implementing Regulation to the Law.

Step	Description of the step	Article
Step 3	<p>The controller must assess if it can use one of the following purposes for cross-border personal data transfer.</p> <ul style="list-style-type: none"> <li data-bbox="245 248 1160 376"> To comply with an obligation under an agreement to which KSA is a party (e.g., trade, security, or diplomatic agreements).  <li data-bbox="245 394 1160 483"> To serve the national interests of the KSA (e.g., national security, economic development, other strategic goals).  <li data-bbox="245 501 1160 591"> Performance of obligations, to which the data subject is a party (e.g. contracts, etc.).  <li data-bbox="245 609 1160 779"> Necessary operations for central processing (e.g., various business operations, including central management operations, administrative functions, and other processes that are important for the controller's functions).  <li data-bbox="245 797 1160 967"> Benefit or a service to the data subject (e.g., services or benefits that might include access to various services, seamless international travel, improved customer experiences, etc.).  <li data-bbox="245 985 1160 1075"> Scientific research and studies.  <p>If the controller can rely on any of the above-mentioned purposes, the controller may proceed to Step 4.</p>	Art. 29 (1) (a) - (c) of the Law, Art. 2 of the Data Transfer Regulations
Step 4	<p>The controller must ensure that the transfer shall not cause any prejudice to national security or the vital interests of the Kingdom³. To comply with this requirement, the controller may:</p> <ul style="list-style-type: none"> <li data-bbox="245 1357 1160 1469">• Review official documents of SDAIA and other Saudi governmental authorities to check if the contemplated transfer is not in breach of their mandatory requirements. <li data-bbox="245 1469 1160 1559">• Apply robust security measures to the personal data subject to the transfer, etc. <p>The controller must also transfer only the minimum data that is necessary to achieve the aim of transfer⁴.</p> <p>If the controller meets the above requirements, the controller may proceed to Step 5.</p>	Art. 29 (2) (a), (c) 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 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 it is not quite clear how this exemption will apply in practice, given that the data minimization is the fundamental principle of the personal data protection. It is expected that SDAIA will additionally clarify this point.

Step	Description of the step	Article
Step 5	<p>The controller needs to identify whether the transfer is to a country or an international organisation with an adequate level of protection, as determined by SDAIA (the country importing the personal data is on the “white list” to be adopted by SDAIA).</p> <p>The controller must proceed to Step 6.1, if:</p> <ul style="list-style-type: none"> • The transfer of the personal data shall be to a country on the “white list”; or • The transfer is necessary to preserve the life or vital interests of the data subject or to prevent, examine or treat disease. <p>The controller must proceed to Step 6.2, if:</p> <ul style="list-style-type: none"> • The transfer of the personal data shall be to the country which is not on the “white list” (including to any country before adoption by SDAIA of the “white list”); or • 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 (2) (b) of the Law
Step 6.1	<p>The controller shall conduct a risk assessment in relation to personal data transfer, if such transfer involves transferring or disclosing sensitive data on a continuous or widespread basis outside the KSA. Please see details on the assessment in the description of Step 7 on page 9 further.</p>	Art. 7 (1) (b) 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**⁵:

Binding Common Rules (BCR): Rules established by the controller, applicable within a group of multinational entities, ensure appropriate protection for personal data transferred outside the Kingdom at a level not less than that prescribed by the Law and Data Transfer Regulations. SDAIA has issued guidance on the use of BCR. 

Standard Contractual Clauses (SCC): SCCs are the provisions to be used by the controller in the agreement regarding transfer of personal data to the other party. Such provisions must be formalized in accordance with a standard form issued by SDAIA. 

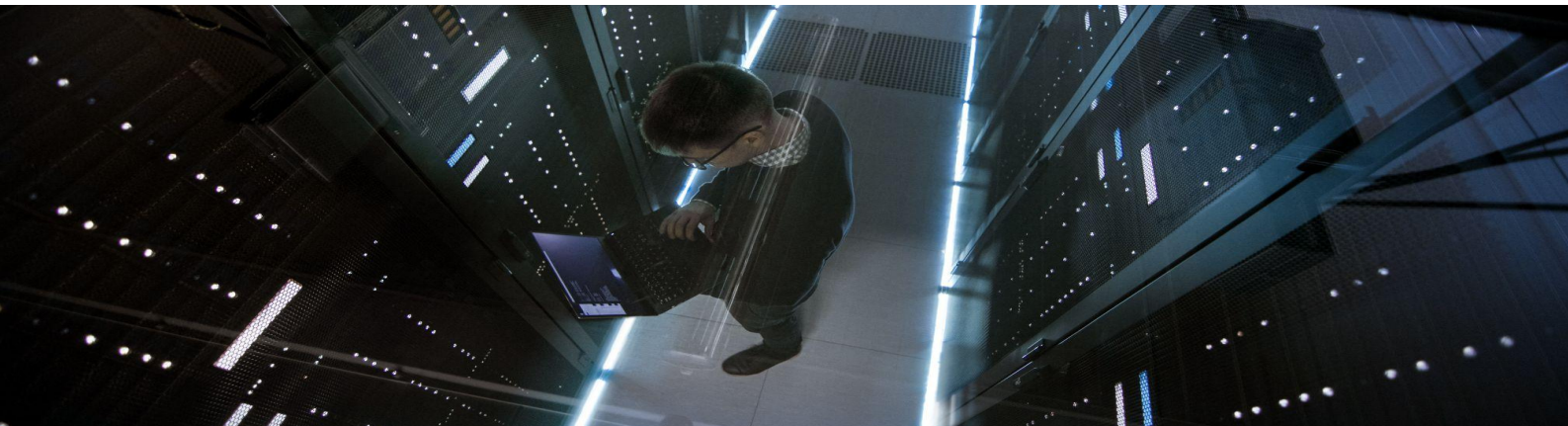
Certification mechanism: This mechanism assumes that the entities authorized by SDAIA will certify the organizations (based outside the Kingdom) to which the data transfers can be made. As of now the rules on the certification mechanism have not yet been established. 

The above safeguards can be applied in cases (exemptions) specified in Art. 4 (2) of the Data Transfer Regulations. **The application of such safeguards is not straightforward and depends on particular cases of cross-border data transfers.** The controller will need to carefully analyze Art. 4 of the Data Transfer Regulations and consider if the data transfer in question can be performed under any of such exemptions and safeguards.

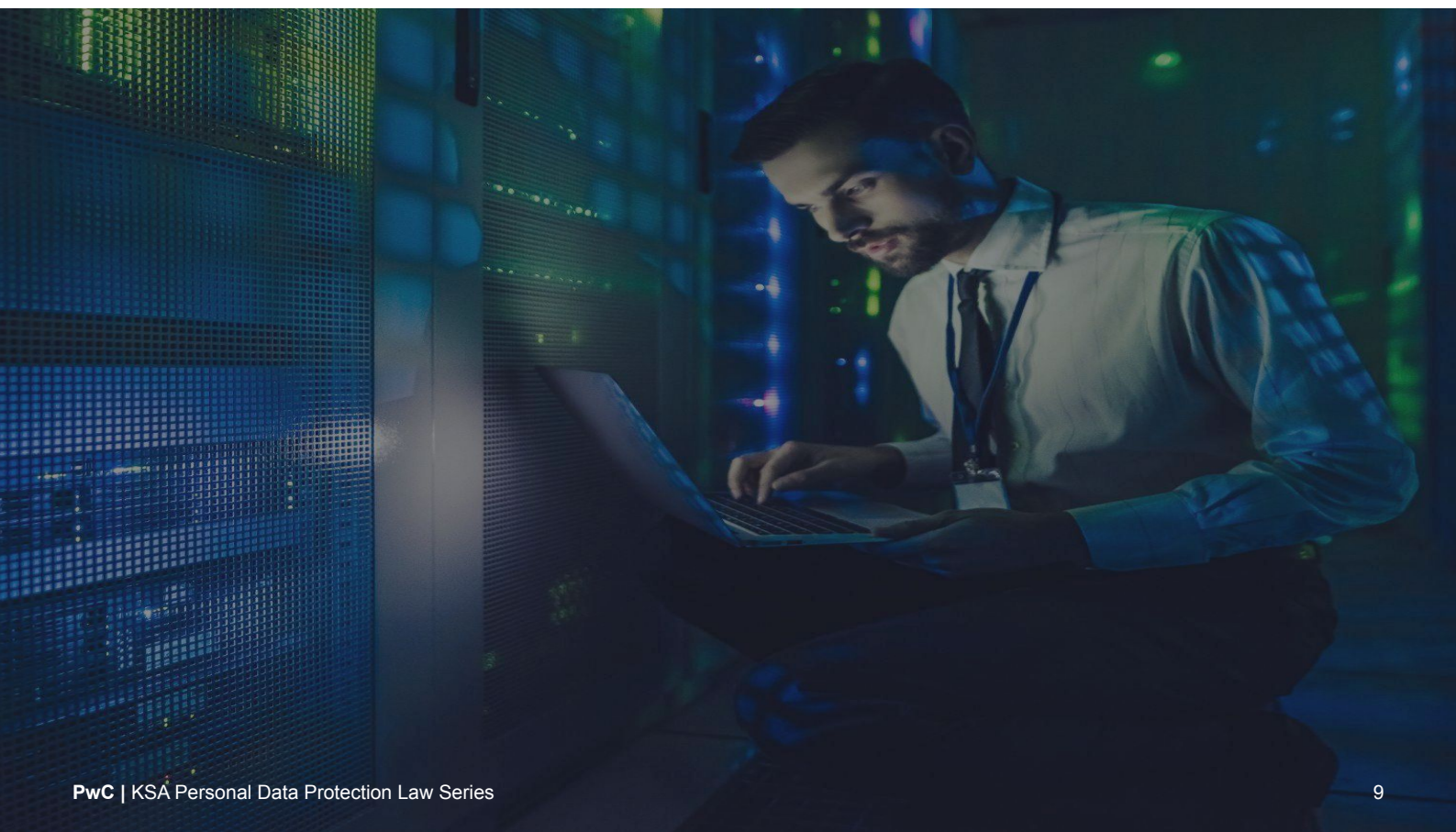
If none of these safeguards may apply - then the personal data **cannot be** transferred outside the Kingdom within the processing activity. If any of the safeguards may apply - then the controller must proceed to **Step 7** (risk assessment).

Art. 4 of the Data Transfer Regulations

⁵ Please note that Art. 4 may be interpreted in such a way, that the safeguards will need to be applied also in cases of transfer of the countries on the “white list”. It is expected that SDAIA will issue a separate guidance document on this topic.



Step	Description of the step	Article
Step 7	<p>The 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.</p> <ol style="list-style-type: none"> 1. The purpose and legal basis for transferring or disclosing personal data to a party outside the Kingdom. 2. A description of the nature of the transfer or disclosure of personal data to a party outside the Kingdom, including the activities involved in processing the data and their geographical scope. 3. The appropriate safeguards and measures implemented for transferring or disclosing personal data to a party outside the Kingdom, and their adequacy in ensuring an appropriate level of protection for personal data not less than that prescribed by the Law and Regulations. 4. The measures used to ensure that the transfer or disclosure of personal data to a party outside the Kingdom is limited to the minimum amount of data required to achieve the intended purposes, in cases not exempted by subparagraph (c) of paragraph (2) of Article (29) of the Law. 5. The potential material or moral effects of transferring or disclosing personal data to a party outside the Kingdom and the likelihood of their occurrence. 6. The measures or controls that will be applied to prevent potential risks to personal data subjects or to mitigate their effects if they occur. <p>After carrying out a risk assessment the controller may proceed with the transfer of personal data.</p>	Art. 7 (1) (a), (2) of the Data Transfer Regulations



Key immediate next steps

Although, there is no one-fit-all approach, the following steps can be taken by your organization in the light of the new rules of the Data Transfer Regulation.

Complete the RoPA in all departments, divisions and business units of your organization to identify all the activities when the personal data is processed (transferred) outside the Kingdom.



Analyze the allowed transfer purposes and safeguards - and consider which of them could be applicable to your cross-border data transfer activities.



Consider possibility of processing personal data only within the KSA, if none of the purposes and safeguards is applicable to your cross-border data transfer activities.



Start preparing data transfer risk assessments in relation to your cross-border data transfer activities.



Prepare a policy or another internal document which will reflect the approach of your organization to the cross-border data transfers (e.g. who in the organization is responsible for the transfers, how the transfers shall be performed, etc.).



Consider approaching SDAIA on clarifying certain points on how to comply with the Data Transfer Regulation.



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](https://www.linkedin.com/in/philmennie) @philmennie



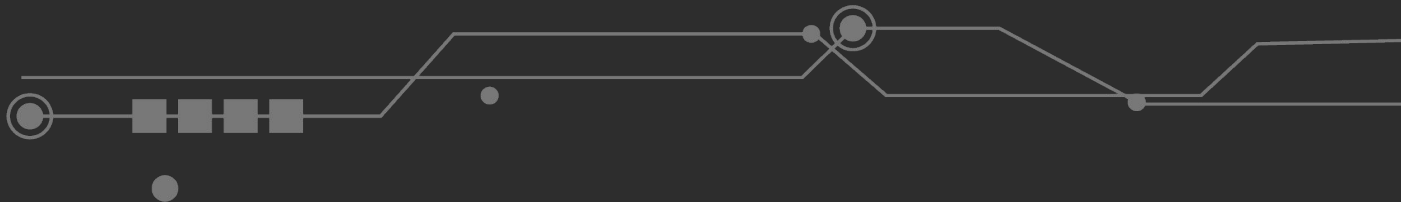
Richard Chudzynski

PwC Data Privacy Legal Leader

+971 56 417 6591

richard.chudzynski@pwc.com

[linkedin.com/in/richardchudzynski](https://www.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.