POLSINELLI | What a law firm should be.™

# International Privacy Law Update

## Introduction

In 2023, India and Saudi Arabia each published new laws and regulations expanding on existing or setting forth new comprehensive data privacy laws. This article summarizes the notable developments in these jurisdictions, specifically focusing on the updated obligations and standards regarding cross-border transfers (i.e., when personal information is transferred from one country to another country). While organizations may already comply with some of these developments by virtue of complying with similarly instituted privacy laws, organizations should take steps to understand fully their obligations to achieve statutory compliance and minimize the risk of legal or financial liability.

## India

After many years in development, the Digital Personal Data Protection Act 2023 (the "Act") was passed by the Indian Parliament in August 2023. The Act is expected to become effective in June 2024 and will supersede relevant provisions in the Information Technology Act, 2000, the Information Technology (Amendment) Act, 2008, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

This Act establishes India among the global powers with a comprehensive privacy law. However, its creation was not without challenges. India faced criticism from data fiduciaries (any organization that determines the data processing purposes and means), notably for the stringent cross-border requirements proposed in earlier drafts of the Act. The previously proposed Digital Personal Data Protection Bill 2022 (the "Bill") seemed to suggest default restrictions on cross-border data transfers, allowing only preselected countries approved by the Central Government, forming a whitelist for such countries. However, this approach significantly limited the number of approved countries, requiring the countries to match or surpass India's level of data protection and be notified by the Central Government of their approval to whitelist the respective country. The Bill also lacked specifics on how the Central Government would select and notify the white-listed countries or the terms and conditions for these transfers, including the transfers of sensitive or critical personal data that potentially affected compliance

and localization requirements.[i] This uncertainty raised concerns among data fiduciaries, given India's significant role in global data processing.

The Act, however, takes a more relaxed stance on cross-border data transfers than did the earlier Bill. As of now, the Act does not restrict the cross-border data transfers unless the Central Government notifies the specific country of the data transfer prohibition.[ii] This significant deviation from the proposed Bill allows data fiduciaries to operate without the fear of noncompliance repercussions. The Act also maintains existing sectoral laws governing industries like banking and telecommunications, preserving their restrictions on cross-border data transfers. Additionally, the Act's extraterritorial reach applies to digital personal data processing outside India if the processing is in connection with any activity referring to offering goods or services to individuals within India, aligning with global privacy laws.

It includes compliance exemptions[iii] for specific circumstances, allowing cross-border data transfers to unapproved countries and the Central Government and its agencies. Those exemptions are as follows:

- Processing of personal data that is necessary for the enforcement of a legal right or claim;
- Prevention, detection, investigation or prosecution of offenses and contraventions under the Indian law;
- Processing of personal data by any court or tribunal or any other body in India for judicial, quasi-judicial, regulatory or supervisory functions;
- Processing of personal data of data principals outside India pursuant to a contract entered into with a foreign entity;
- Processing pursuant to legally approved mergers, demergers, acquisitions and other such arrangements between data fiduciaries; and
- Processing personal data to ascertain the financial position of a defaulter to a financial institution.

Ultimately, the Act presents a broad foundation, outlining the basics of a comprehensive privacy law in India. The implementation and enforcement of the Act is expected to emerge from the Central Government in the form of rules and regulations. The Data Protection Board of India will oversee compliance with this Act and issue corrective orders and penalties for noncompliance.

*Key Takeaways for Organizations:*

While no specific timelines for compliance have been provided, organizations should:

- Regularly review and access their data flows out of India;
- Ensure that proper data transfer agreements are in place;
- Regularly check the list of restricted countries, once it is made available by the Central Government, to avoid noncompliance penalties; and
- Be aware that noncompliance penalties could reach up to rupees 2.5 billion (approx. $30 million).

## Saudi Arabia

On September 7, 2023, the Saudi Data and Artificial Intelligence Authority issued both the Implementing Regulation of the Personal Data Protection Law (the "Implementing Regulation") and the Regulation on Personal Data Transfer outside the Kingdom (the "Transfer Regulation," and collectively with the Implementing Regulation, the "Regulations") to clarify and supplement the Kingdom of Saudi Arabia ("KSA") Personal Data Protection Law ("PDPL").[iv] Together, the PDPL and Regulations are designed to parallel other international privacy laws and establish comprehensive data protection standards within KSA.

*Cross-Border Transfers*

Article 29 of the PDPL and the Transfer Regulation prescribe how data controllers[v] can legally transfer personal data[vi] outside the KSA or to a party outside the KSA. Under Article 29, data controllers may initiate such transfer if the transfer is (1) related to performing a contractual obligation where the KSA is a party, (2) to serve the interests of the KSA, (3) to perform an obligation where the data subject is a party to such obligation *or* (4) to fulfill the purposes in the Regulations.[vii] Except in cases of extreme necessity or to prevent injuries or disease, Article 29 further requires that data transfers are only permissible when (a) the transfer will not prejudice national security or the vital interests of the KSA, (b) there is an adequate level of protection outside the KSA, and such adequacy is established by an assessment performed by a competent authority in the KSA, *and* (c) the personal data transferred is limited to the minimum amount necessary.[viii] Assuming a data controller satisfies these requirements, a data controller may legally transfer such personal data outside the KSA.

Markedly, the Transfer Regulation expands on Article 29 by describing in further detail the criteria and procedures for cross-border transfers. While the Transfer Regulation reinforces some of Article 29's requirements (e.g., by ensuring data transfers will not impact national security), the Transfer Regulation also requires data controllers to ensure the transfer does not adversely affect the level of privacy afforded to personal data.[ix] For instance, the transfer must not compromise a person's right to withdraw consent to data processing or a data controller's ability to notify data subjects in case of a data breach.[x] Further, the Transfer Regulation expands on the purposes for a transfer in Article 29, paragraph 1 by allowing data controllers to transfer personal data if (1) the transfer will enable the data controller to "carry out its activities," (2) the transfer will provide a service or benefit to the data subject, *or* (3) the transfer is for conducting scientific research.[xi] Moreover, the Transfer Regulation requires data controllers to perform risk assessments for transfers where the jurisdiction does not have adequate levels of protection or consistent transfers of sensitive data.[xii]

Additionally, the Transfer Regulation requires a competent authority (to be determined later by the Council of Ministers) to evaluate the protections of personal data outside the KSA based on enumerated criteria and recommend adequacy decisions based on such evaluations,[xiii] similar to the EU-U.S. adequacy decision published in July 2023. These evaluations help data controllers ensure the personal data is transferred to a jurisdiction with an adequate level of protection to comply with Article 29 of the PDPL.

Finally, the Transfer Regulation provides some exceptions where a jurisdiction does not have adequate protections. If a jurisdiction does not have the adequate levels of protection, the data controller may still transfer the personal data *provided* the other jurisdiction does not prejudice the privacy of the personal data subject or the data controller's capability to implement appropriate safeguards.[xiv] In cases where a jurisdiction does not have the adequate levels of protection or a data controller cannot implement the appropriate safeguards, the KSA allows data controllers to conduct transfers so long as (1) the transfer is necessary for performing obligations where the data subject is a party, (2) the data controller is a public entity and the transfer is necessary to protect KSA's national security or for the public interest, (3) the data controller is a public entity and the transfer is necessary to investigate or detect crimes, *or* (4) the transfer is necessary to protect the vital interests of a data subject who cannot be contacted.[xv] However, these exemptions are not applicable and a data controller must immediately stop or prevent any such transfers if (a) the transfer negatively affects KSA's national security or vital interests, (b) there is a high risk to a data subject's privacy based on the results of a risk assessment, (c) the adopted appropriate safeguards no longer apply, *or* (d) the data controller cannot enforce the appropriate safeguards.[xvi]

*Compliance and Consequences*

Data controllers have a one-year grace period ending on September 14, 2024, to comply with the PDPL and accompanying Regulations. Notably, the PDPL and Regulations contain other provisions in addition to cross-border transfers that address, among other things, data subject rights, information security standards, and data controller obligations regarding processers. Deliberately violating the PDPL and its Regulations with the intent to harm could result in imprisonment for two years or a fine of 3,000,000 riyals (or approximately $800,000).[xvii] Other failures to comply with the PDPL and its Regulations risk fines of up to 5,000,000 riyals (or approximately $1.3 million), which may be doubled for repeat offenders.[xviii]

*Key Takeaways for Organizations:*

Before the grace period ends in 2024, organizations should:

- Review data processing activities and privacy compliance programs;
- Update activities and programs to comply with the PDPL and its Regulations as necessary;
- Review or audit arrangements with processors/sub-processors to help ensure compliance; and
- Educate employees on obligations for the organization and themselves.

---

[i] The Bill did not define the terms *sensitive personal data* and *critical personal data*.
[ii] The Digital Personal Data Protection Act 2023, Bill No. 113-C of 2023, Chapter IV § 16(1).
[iii] The Digital Personal Data Protection Act 2023, Bill No. 113-C of 2023, Chapter IV § 17(1).
[iv] Royal Decree No. M148 of 05/09/1444H, M/19 of 9/2/1443H (2023).

[v] "Controller" is defined as "[a]ny Public Entity, natural person or private legal person that specifies the purpose and manner of Processing Personal Data, whether the data is processed by that Controller or by the Processor." *Id.* at art. 1(18).

[vi] "Personal Data" is defined as "[a]ny data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual, including name, personal identification number, addresses, contact numbers, license numbers, records, personal assets, bank and credit card numbers, photos and videos of an individual, and any other data of personal nature." *Id.* at art. 1(4).

[vii] *Id.* at art. 29(1).

[viii] *Id.* at art. 29(2).

[ix] The Implementing Regulations of the Personal Data Protection Law, Regulation on Personal Data transfer outside the Kingdom, chap. 1, art. 2 (2023).

[x] *Id.*

[xi] *Id.*

[xii] *Id.* at chap. 4, art. 8.

[xiii] *Id.* at chap. 2, art. 3.

[xiv] *Id.* at chap. 3, art. 5.

[xv] *Id.* at chap. 3, art. 6.

[xvi] *Id.* at chap. 3, art. 7.

[xvii] Royal Decree No. M148 of 05/09/1444H, M/19 of 9/2/1443H (2023), art. 35(1).

[xviii] *Id.* at art. 36(1).