Global Data and Cyber Handbook - India

Data localization and regulation of non-personal data

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# Are there data localization/data residency or other types of laws that may require the retention and storage of data in the local jurisdiction, or prohibit the transfer of data out of the jurisdiction?

*Last review date: 20 December 2024*

**Yes**

While the DPDP does not provide specific data localization requirements, it recognizes sector-specific laws that may have requirements to localize different categories of data, which may include personal data.

☒  Other laws that may require the retention and storage of personal data (including, for example, where such data is part of another type of record or dataset) in the local jurisdiction or otherwise prohibit the transfer or disclosure of the personal data outside of the local jurisdiction:

☒  tax or financial record laws

☒  other

As per a [notification dated 6 April 2018](https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&amp;amp;amp;amp;Mode=0) issued by the Reserve Bank of India (RBI), India's central banking regulatory, all licensed banks and payment system providers must ensure that all data relating to payment systems operated by them are stored in a system located in India. Such data includes full end-to-end transaction details and any information collected, carried, or processed as a part of a message or payment instruction. The notification, however, clarifies that where a transaction has a foreign element, data pertaining to such transaction may be stored in the relevant foreign country *in addition* to being stored in India.

Further, the Securities Exchange Board of India (SEBI) has issued an advisory for financial sector organizations such as merchant banks, credit rating agencies, STP service providers, debenture trustees, depositary participants, and other financial institutions that use Software as a Service (SaaS) based solutions for managing their governance, risk and compliance functions. Per this advisory, certain critical data sets such as credit and liquidity risk data, market risk data, system and sub-system information, supplier information, system configuration data, audit/internal audit data, network topography and design, are required to be stored in India.

More recently, the SEBI has issued a Framework for Adoption of Cloud Services by regulated entities. Under this framework, if regulated entities engage cloud service providers to conduct their business functions and if data pertaining to regulated entities is on the cloud in any form, the same is required to be stored within the legal boundaries of India. However, if the regulated entity has a foreign parent entity, the original data can be made readily accessible in India, i.e., a copy of such data that is on the cloud may be stored abroad.

Separately, the Insurance Regulatory and Department Authority of India (Maintenance of Insurance Records) Regulations, 2015, require insurance providers to store data related to policies and claim records of insurers to be stored on systems in India (even if this data is held in an electronic form).

Additionally, while Section 128 of the Companies Act, 2013 requires every company to prepare and store books of account, other relevant books and papers, and financial statements at its registered office for each financial year, on 5 August 2022, the Ministry of Corporate Affairs amended this rule so that all such relevant books and papers maintained in an electronic mode should remain accessible in India, at all times.

Further, the Ministry of Electronics and Information Technology's directions on information security practices, procedure, prevention, response and reporting of cyber incidents dated 28 April 2022 (in force since 28 June 2022), read with the frequently asked questions released on these directions, require service providers offering services to users in the country to enable and maintain logs and records of financial transactions within India.

# Does law or regulation impose mandatory requirements to share or make accessible non-personal data?

*Last review date: 20 December 2024*

☒  Obligation for private organizations to share or make accessible other non-personal data

***If so, please provide brief details of the relevant law or regulation.***

There is no overarching law requiring the sharing of non-personal data across sectors. However, certain sectoral regulators may require regulated entities to share or make accessible non-personal data relating to regulated activities.

# What specific obligations do these data-sharing rules impose on private organizations?

*Last review date: 20 December 2024*

Obligation to share data on request

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.