Global Data and Cyber Handbook - Vietnam

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: 2 January 2025*

Yes.

a)   data localization / data residency laws that mandate retention of personal data or a copy thereof in the local jurisdiction (include whether copies or the original data may also be stored outside of the jurisdiction):

The Cybersecurity Law and Decree No. 53 impose data localization obligations on onshore and offshore providers of telecommunications services, internet services, and value-added services in cyberspace ("**Cyberspace Service Providers – CSP**"). The specific triggering conditions and requirements are as follows:

|  |  |  |
| --- | --- | --- |
|   | **Domestic entities** | **Offshore entities** |
| **Conditions** | **(A1)** Being a CSP, **AND** **(A2)** Collecting, exploiting, analyzing, and/or processing data on personal information, data on the relationship of the service users, and data created by service users in Vietnam ("**Regulated Data**"). | **(B1)** Being a CSP (specific services/business lines are provided) **(B2)** Collecting, exploiting, analyzing, and/or processing Regulated Data **(B3)** Its services are used to commit acts violating the law on cybersecurity for which the MPS A05 has notified and requested coordination, prevention, investigation and handling in writing **(B4)** The offshore entity fails to comply, complies insufficiently or prevents, hinders, neutralizes or invalidates cybersecurity protection measures taken by the specialized force in charge of cybersecurity protection, **AND** **(B5)** The MPS issues a decision requesting data storage and the establishment of a branch or representative office in Vietnam. |
| **Requirements** | Store the above data in Vietnam. | Store the above data in Vietnam; **AND** Set up either a representative office or a branch in Vietnam. |

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

*Last review date: 2 January 2025*

☒  Obligation for public sector organizations to share or make accessible non-personal data

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

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

☒  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.***

According to the Data Law, State authorities are responsible for announcing the list of open data and organizing its public disclosure for organizations and individuals to exploit, use and share. Open data is defined as data that any agency, organization, or individual can access, share, exploit, and use as needed. State authorities must make certain information publicly available or provide on-demand access to citizens in relation to their right to access information under the Information Access Law.

The Medical Law permits access to medical records (covering personal and non-personal information) during and after treatment by different organizations and individuals under certain conditions. For example, representatives of State agencies in charge of health, investigative agencies, procuracies, courts, health inspectors, forensic organizations, forensic psychiatrists, and patients' lawyers are allowed to access and provide medical records to perform their tasks in accordance with relevant laws.

Law 2024 on Credit Institutions and Decree No. 117/2018/ND-CP on the protection of confidentiality and provision of client information of credit institutions and foreign banks’ branches oblige credit institutions and foreign bank branches to provide client information to State authorities, organizations and individuals upon a lawful request. Client information may include non-personal information if all personal identifiers are removed from the dataset.

The Cybersecurity Law and Decree No. 53 empower competent cybersecurity authorities to collect electronic data from any organizations and individuals to serve the investigation and handling of acts that violate national security, social order and safety, and the legitimate rights and interests of agencies, organizations and individuals in cyberspace.

The Data Law mandates organizations and individuals to provide data to State agencies upon request, even without the data subject's consent, in the following specific circumstances: emergency response, threats to national security that are yet to be a state of emergency, disasters, and prevention and control of riots and terrorism.

There are other laws generally requiring organizations and individuals to comply with lawful requests from State authorities, which might necessitate the disclosure of data (e.g., in relation to the investigation of a crime).

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

*Last review date: 2 January 2025*

☒  Obligation to share data on request

☒  Obligation to share data proactively

☒  Obligation to (re)design products or services to facilitate data accessibility

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.