Global Data and Cyber Handbook - Vietnam

Security Requirements and Breach Notification

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

# Do data privacy laws or regulations impose obligations to maintain information security controls to protect personal data from unauthorized access or processing?

*Last review date: 2 January 2025*

Yes.

☒  general obligation to take appropriate / reasonable technical, physical and/or organizational security measures

☒  obligation to take specific security measures e.g., encryption

# Do other laws or regulations impose obligations to protect systems from cyberattack?

*Last review date: 2 January 2025*

Yes.

☒  network information security requirements (broader than telecommunications)

☒  health regulatory requirements

☒  financial services requirements

☒  telecommunication requirements

☒  providers of critical infrastructure

☒  other

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

Cyber information security laws stipulate several requirements for the protection of cyber information security for both critical and non-critical information systems. Enterprises providing services in cyberspace in Vietnam are also responsible for implementing different cybersecurity measures such as alerting cybersecurity risk, developing an incident response plan, implementing appropriate response measures in light of an actual incident, reporting, and cooperation. Banking regulations also prescribe protection measures in relation to information safety and cybersecurity. Law 2023 on Telecommunications also requires compliance with cybersecurity laws when rendering telecom services. Law 2023 on Medical Examination and Treatment also makes general reference to the obligation to apply security measures in medical establishments, which can be broadly interpreted to necessitate the adoption of cybersecurity measures to protect patients' health-related information. Information safety and security, which can potentially be infringed by a cybersecurity incident, are also regulated under other domains of laws such as consumer protection, e-commerce, information technology, etc.

# Has there been regulatory activity – including enforcement action, investigations, regulatory guidance or other public statements by the regulator – relating to cybersecurity by the following regulators in the last 12 months?

☒  Data privacy

☒  network information security

# Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?

*Last review date: 2 January 2025*

Yes.

Data breach is currently regulated under different general and sector-specific regulations. Data breach can be either a personal data violation under the PDPD, a cybersecurity incident or cyber information security incident respectively per cybersecurity or cyber information security laws, or an attack on the information system that poses a risk to the consumer information's security and safety pursuant to consumer protection regulations, etc. The reporting entity, deadline, and procedure also vary across pieces of legislation and regulations.

# Controllers/Owners have to notify:

*Last review date: 2 January 2025*

☒  data protection authorities

The data protection authorities to whom a report must be submitted vary across sectors and are determined by the specific legal documents that grant them jurisdiction.

☒  affected individuals

Article 41.1.c of the LOCS generally requires enterprises providing services in cyberspace in Vietnam to notify users of information breaches or risks of such breaches. However, the LOCS and its implementing Decree (i.e., Decree No. 53) do not provide details on the timeline and method of notification to users, and as a result, this requirement has not been actively enforced.

Furthermore, a controller may need to notify impacted data subjects of a personal data breach to ensure their right to know under the PDPD.

☒  other

Cyber information security laws further require an incident report to be made to members of the incident response network.

# Processors/Agents have to notify:

*Last review date: 2 January 2025*

☒  controller

Under the PDPD, a processor has to notify its controller as soon as possible upon being aware of a personal data violation. An information system operator under cyber information security laws is tasked with reporting an incident to its administrator within five days after detecting the incident.

☒  data protection authorities

Where the laws do not differentiate between a processor and controller, the entity responsible for data processing (which can be a processor under the PDPD) must notify a data breach to competent data protection authorities.

☒  affected individuals

Article 41.1.c of the LOCS generally requires enterprises providing services in cyberspace in Vietnam to notify users of information breaches or risks of such breaches. However, the LOCS and its implementing Decree (i.e., Decree No. 53) do not provide details on the timeline and method of notification to users, and as a result, this requirement has not been actively enforced.

☒  others

Cyber information security laws further require an incident report to be made to members of the incident response network.

# Are there any additional sector-specific or non-personal data security breach notification requirements?

*Last review date: 2 January 2025*

Yes.

☒  other

In the context of e-commerce websites, when an information system is hacked and there is a risk of loss of consumer information, the organization storing such information must notify the authorities within 24 hours after detecting the breach.

In the context of banking, credit institutions (with the exception of people's credit funds and microcredit institutions), branches of foreign banks and intermediary payment service providers must report cybersecurity incidents to the State Bank of Vietnam (via email: antt@sbv.gov.vn) within 24 hours of the incident being detected and within five working days after the completion of the incident resolution.

In the context of consumer protection, traders are obliged to notify a competent authority within 24 hours after the detection of an attack on the information system that poses a risk to the security and safety of consumer information.

In the context of cyber information security, operators of information systems must notify an incident to various incident response agencies within five days after detecting a non-serious cyber information security incident (e.g., incidents not involving State secrets).

In the context of cybersecurity, enterprises providing services in cyberspace in Vietnam are required to notify users and report to the specialized cybersecurity force in the event of an actual or potential leak or loss of user data.

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.