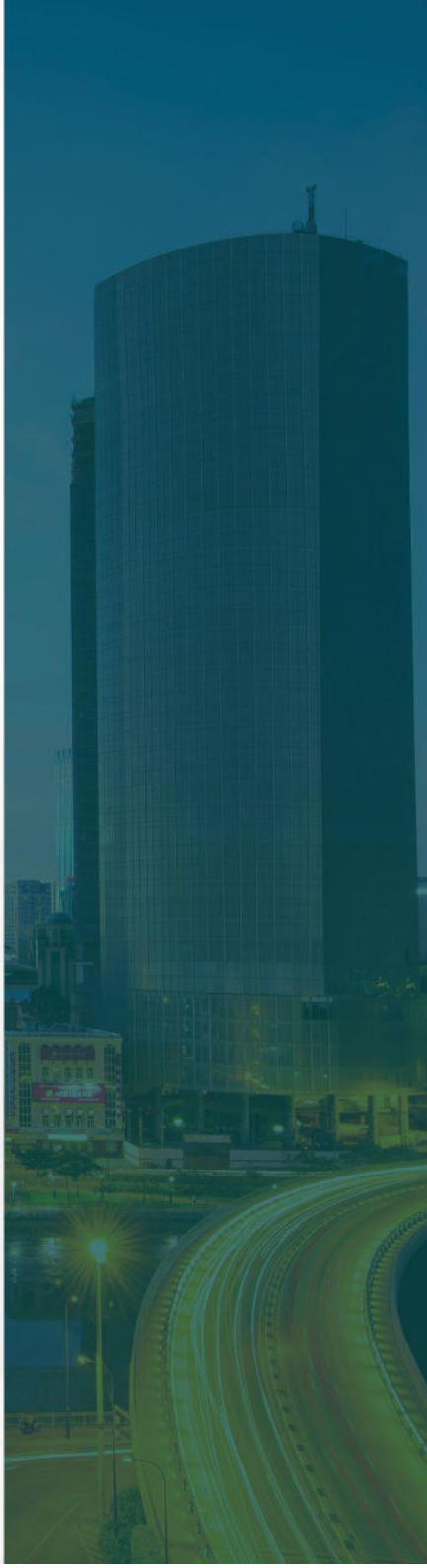
DFDL

LEGAL ALERT

Navigating Vietnam's Personal Data Protection Decree: Five Frequently Asked Questions



SHARE • INFORM • LEARN

CONTENTS

1. What does "*Personal Data*" mean under the PDPD? 5

2. What are the key roles (and associated responsibilities) in relation to the processing of personal data under the PDPD? 6

3. For a cross-border personal data transfer, who must conduct a transfer impact assessment? 8

4. How long must controllers and processors keep data and when should they delete it? 10

5. I am using offshore technology services (such as cloud services). Which specific considerations should I take into account to ensure compliance with the PDPD requirements? 11

Navigating Vietnam's Personal Data Protection Decree: Five Frequently Asked Questions

Your quick guide to burning questions you might have about the new PDPD. Who is affected? What do you need to do? Is it compatible with the use of offshore technology such as cloud storage services? And more.

Vietnam's first-ever comprehensive legal framework dedicated to personal data protection introduces new rules that capture a wide range of entities.

The new rules – officially titled Decree No. 13/2023/ND-CP and referred to as the Personal Data Protection Decree (or **PDPD**) – were issued on 17 April 2023 and took effect from 1 July 2023.

The PDPD covers:

- any agency, organization, or individual – whether local or foreign – engaged in the collection and processing of Vietnamese personal data
- onshore and offshore personal data processing and transfers (anyone transferring Vietnamese citizens' personal data to a foreign country must submit an offshore transfer impact assessment dossier to the competent State authority).

The PDPD follows hot on the heels of another key new cyberspace regulation in Vietnam, Decree 53 dated 15 August 2022 on the Law on Cybersecurity (12 June 2018). Understandably, it has triggered a range of queries from potentially affected clients, not least those who use, or are considering the use of, offshore technology like cloud storage services for the handling of their data.

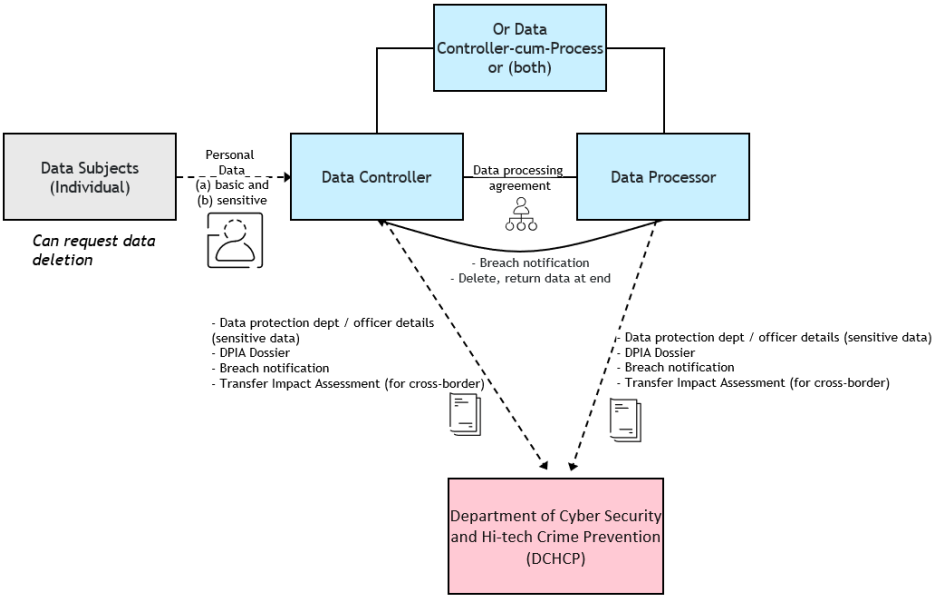
What kind of data is covered, what are the notification and disclosure duties for data controllers and processors, when does data need to be deleted, and is the

PDPD even compatible with the use of technology such as offshore cloud services at all?

This legal alert briefly addresses each of these questions. Many of the PDPD's provisions are cast in broad terms – they and their intended implementation are not necessarily clear in all respects. Further guidance on these matters is likely to be forthcoming. But we consider that a path for compliance with the PDPD can nevertheless be navigated in the meantime, including for the use of offshore cloud storage services.

Of course, the specifics of your circumstances are important. If you would like to discuss those circumstances and your particular path, please contact Kevin Hawkins, Partner at kevin.hawkins@dfdl.com.

For further information on this subject, we recommend referring to other articles available "*Vietnam: Data-Driven Duties*".



1. What does "*Personal Data*" mean under the PDPD?

Under the PDPD, "personal data" refers to any information in the digital environment that relates to a specific individual or aids in the identification of a particular person.

Personal data encompasses:

- basic personal data, and;
- sensitive personal data.

Sensitive personal data is defined as personal data associated with an individual's privacy that, when violated, will directly affect an individual's legitimate rights and interests. The PDPD provides a non-exhaustive list of examples:

- Political and religious opinions;
- Health condition and personal information stated in a health record, excluding information on blood group;
- Information about racial or ethnic origin;
- Information about genetic data related to an individual's inherited or acquired genetic characteristics;
- Information about an individual's own biometric or biological characteristics;
- Information about an individual's sex life or sexual orientation;
- Data on crimes and criminal activities collected and stored by law enforcement agencies;
- Information on customers of credit institutions, foreign bank branches, payment service providers, and other licensed institutions, including customer identification as prescribed by law, accounts, deposits, deposited assets, transactions, organizations, and individuals that are guarantors at credit institutions, bank branches, and payment service providers;
- Personal location identified via location services;
- Other specific personal data as prescribed by law that requires special protection.

2. What are the key roles (and associated responsibilities) in relation to the processing of personal data under the PDPD?

Data Controllers and Data Processors have duties and responsibilities relating to notification, protection, retention, deletion and setting policies for collecting and processing data. Those who control and process data (Data Controller-cum-Processors) must follow both sets of rules.

Data Controllers

"Data Controllers" are organizations or individuals who determine the purpose and means of personal data processing. It is the Data Controller who has the higher level of obligation under the PDPD and is ultimately accountable to Data Subjects.

Data Controllers are responsible for:

- Notifying Data Subjects (i.e. individuals who are identifiable by their personal data) of certain information about the processing of their personal data;
- Ensuring Data Subjects' requests pursuant to their rights under the PDPD (eg to restrict, access, object, correct, or delete their data) are received and addressed;
- Implementing appropriate technical and organizational measures to ensure personal data protection;
- Recording and storing system logs of the personal data processing;
- Selecting a Data Processor in accordance with a clear mandate utilizing appropriate safeguards;
- Bearing the burden of proving Data Subjects' consent to, or other lawful basis for, data processing in the event of a dispute;
- Issuing a personal data protection policy;
- For the processing of sensitive personal data, designating (and notifying the Department of Cyber Security and Hi-tech Crime Prevention under the Vietnamese Ministry of Public Security (DCHCP) of the details of) a data protection department and data protection officer;

- Preparing, retaining, and sending a copy of a data protection impact assessment dossier (**DPIA Dossier**) to the DCHCP within 60 days from commencement of, or changes to, personal data processing activity (**Commencing Date**);
- In the case of a personal data breach, notifying the personal data breach to the DCHCP no later than 72 hours after the occurrence of the breach;
- Storing personal data in a form appropriate to its operations with measures to protect personal data in accordance with the law.

Data Processors

"Data Processors" are organizations or individuals engaged under a contract with a Data Controller to process personal data for and in accordance with the instructions of that Data Controller. They assume responsibility for:

- Receiving and processing personal data in accordance with agreements with the Data Controller;
- Establishing a personal data protection policy, in compliance with the PDPD, to implement in their operations;
- In the case of processing sensitive personal data, designating a data protection department and data protection officer and notifying the DCHCP of their details;
- Preparing, retaining, and sending a copy of the DPIA Dossier to the DCHCP within 60 days from the Commencing Date;
- Notifying the Data Controller of any personal data breach, as soon as possible after becoming aware of it;
- Deleting or returning to the Data Controller all personal data when the relevant data processing arrangement ceases;
- Storing personal data in a form appropriate to its operations with measures to protect personal data in accordance with the law.

Data Controller-Cum-Processors

"Data Controller-Cum-Processors" are organizations or individuals that simultaneously act as Data Controllers and Data Processors. They must fulfill all the obligations of both Data Controllers and Data Processors.

3. For a cross-border personal data transfer, who must conduct a transfer impact assessment?

A Transfer Impact Assessment is required for cross-border personal data transfers, completed by the personal data transferor and containing key prescribed information.

Under the PDPD, it still remains quite possible to transfer personal data to another country (that is, a server or other store of the data located outside of Vietnam). However, as with all personal data processing activity, in order for such a transfer to be compliant with the PDPD's requirements, the party transferring personal data abroad, who may be any of the Data Controller, Data Processor, or Data Controller-cum-Processor ("**Personal Data Transferor**"), must:

- Prepare, retain, and send a copy of a Transfer Impact Assessment dossier for cross-border data transfer to the DCHCP within 60 days after processing the data, with the application form provided in the PDPD (that is, Form No. 06). To provide further clarification, even though there is currently no specific official guidance available for the PDPD, unofficial guidance from Vietnamese state authorities suggests that the process of creating a Transfer Impact Assessment dossier is separate from that of a DPIA dossier. When it comes to the transfer of personal data abroad, it is therefore considered necessary to prepare both a DPIA dossier and a Transfer Impact Assessment dossier. The responsibility for preparing DPIA dossiers lies with the relevant party, as applicable to the circumstances of their handling of personal data. Conversely, the preparation of a Transfer Impact Assessment dossier is the sole responsibility of the Personal Data Transferor (i.e. one of the Data Controller, Data Controller-Cum-Processor or Data Processor, or more than one of them if they are mutually involved in the cross-border data transfer);
- Send a notification to the DCHCP after the successful transfer of data.

The Transfer Impact Assessment dossier must include the following key information:

- Contact information and particulars of the transferor and transferee involved in the data transfer;
- Contact details of a representative of the transferor;
- A comprehensive description and explanation of the objectives behind the transfer of personal data abroad;
- Detailed information about the type of personal data intended to be transferred abroad;
- A description and explanation of how all parties will adhere to regulations pertaining to personal data protection during the transfer process;
- An assessment of the potential impact of processing personal data abroad, including identification of any potential undesired consequences or damages that may arise, along with measures for mitigating such outcomes;
- The documented consent of the Data Subject from whom the data is being collected, along with evidence of their awareness of means of recourse in case of any problems;
- A document outlining the obligations and responsibilities of both the transferor and transferee in processing the transferred data.

Importantly, the PDPD grants the Ministry of Public Security the right to inspect and audit data handlers' personal data management practices and policies (including cross-border transfers of personal data) once per year (or more often if considered necessary).

There is currently no specific guidance on how to prepare the Transfer Impact Assessment and notifications of successful data transfers in the circumstances of cross-border personal data transfers in regular, unidentifiable flows (as may occur in the context of using cloud services or automatic e-systems, for example). However, according to unofficial guidance from the relevant state authority, the Transfer Impact Assessment dossier and notification process should be conducted once only for specific transfer methods and types of personal data. If there are changes in the types of data being transferred abroad and/or the methods of data

transfer, the Transfer Impact Assessment dossier must be updated accordingly and submitted to the DCHCP. In the circumstances of using these sorts of services, we would typically expect the Vietnam-based customer to be the Personal Data Transferor (as they, and not the service provider, would usually determine all aspects of the data transfer).

4. How long must controllers and processors keep data and when should they delete it?

Data Controllers / Processors should retain data for the duration appropriate to process it and must delete it upon request by the Data Subject

- **Data retention**: there are no specific regulations (as of September 2023) regarding the retention period of personal data. The law only specifies that personal data should be retained for a duration that is appropriate for the purposes of data processing. Additional guidance is expected soon;
- **Data deletion:** A Data Subject can at any time require a Data Controller or Data Controller-Cum-Processor to delete their personal data. By law, data deletion must be completed within 72 hours of the Data Subject's request. The legal framework for administrative sanctions in case of violations of personal data protection regulations, particularly concerning the breach of data deletion requirements, is still in its drafting phase and is expected to be enacted by the end of Q4 2023 or within Q1 2024. Under the current draft, the proposed range of monetary penalty is VND 60M-80M (approx. USD 2,550-USD3,400).

5. I am using offshore technology services (such as cloud services). Which specific considerations should I take into account to ensure compliance with the PDPD requirements?

The PDPD requirements apply even if a foreign service provider is used to collect & process personal data – including using technology like the cloud.

Vietnamese entities that engage foreign service providers for services that involve the collection or processing of personal data must adhere to the requirements set forth in the PDPD. Clearly, this does require an awareness of the sorts of additional obligations briefly outlined in this article, and the taking of additional steps (in concert with your service provider, where relevant) to meet those obligations, relative to the position prior to the PDPD coming into effect. However, in our view it is quite possible to steer a compliant path.

If the services you procure necessitate the transfer of personal data to foreign countries, the Personal Data Transferor (that is, you as a Vietnam-based client) must fulfill the following obligations:

- Establish a mutual agreement (in writing) between the relevant entities transferring and receiving personal data of Vietnam citizens, expressing the commitment and responsibilities of each party about the processing of personal data;
- Ensure the proper implementation of the obligations of the parties, commensurate with their respective roles in data processing activities;
- Ensure the instances of services from foreign countries are consistent with the cross-border personal data transfer instances under the DPIA Dossier submitted to the DCHCP;
- Obtain explicit consent from the Data Subject for the transfer of their data abroad;
  - Consent must be expressed in a clear and specific manner in writing, verbally, by ticking the consent box, by consent syntax via message, by selecting consent settings, or by any other form capable of expressing agreement in a similarly clear and specific manner.

- Prepare, retain, and send a copy of a Transfer Impact Assessment dossier for cross-border data transfer to the DCHCP. Update and resubmit the Transfer Impact Assessment dossier if there is any material change to the data transfer/processing practices (and the existing dossier is therefore inaccurate). To reiterate, in addition to preparing the Transfer Impact Assessment dossier, you, as a Data Controller or Data Controller-cum-Processor, are still required to compile and submit a separate DPIA dossier.

Any proposed arrangements for cross-border transfer of personal data should also consider data localization requirements (in certain cases) as stipulated in Decree 53/2022/ND-CP issued by the Government of Vietnam on 15 August 2023. For more on this, please see "*Vietnam: New Decree 53 details Certain Provisions in the Law on Cybersecurity*"

The information provided in this legal alert is for information purposes only and is not intended to constitute legal advice. Legal advice should be obtained from qualified legal counsel for all specific situations.

Excellence. Creativity. Trust

Since 1994

BANGLADESH | CAMBODIA* | INDONESIA*| LAO PDR | MALAYSIA* | MYANMAR
PHILIPPINES* | SINGAPORE | THAILAND | VIETNAM
*DFDL collaborating firms