
AUGUST 2022

AUTHORED BY

Dominic Paulger

Policy Manager (APAC), Future of Privacy Forum

PROJECT LEAD

Dr. Clarisse Girot

Honorary Senior Fellow, Asian Business Law Institute

CONTRIBUTORS

Linh Tong Khanh

Policy Analyst, Institute for Policy Studies and Media Development

Waewpen Piemwichai

Attorney-at-Law, Tilleke & Gibbins

ACKNOWLEDGEMENTS

This Report benefitted contributions and editing support from Catherine Shen.

DISCLAIMER

Views expressed in this Report are not necessarily those of the Project Lead, the Asian Business Law Institute (ABLI), the Singapore Academy of Law (SAL), or the Future of Privacy Forum (FPF). While every effort has been made to ensure that the information contained in this Report is correct, the Authors, the Project Lead, ABLI, SAL, and FPF disclaim all liability and responsibility for any error or omission in this Report, and in respect of any thing, or the consequences of any thing, done or omitted to be done by any person in reliance, whether wholly or partially, upon the whole or part of the consequences of this Report.

TABLE OF CONTENTS

1. INTRODUCTION	1
2. CONSENT AND PRIVACY SELF-MANAGEMENT IN EXISTING LAWS AND REGULATIONS	3
2.1. Health sector	5
2.2. Credit sector	5
3. CONSENT AND PRIVACY SELF-MANAGEMENT IN THE DRAFT PDP DECREE	5
4. CONDITIONS FOR CONSENT.....	6
4.1. Definition and forms of consent	6
a. Consent in e-commerce	6
b. Consent to receive advertising or marketing communications.....	7
c. Consent in the Draft PDP Decree	7
4.2. Withdrawal of consent	8
a. Existing data protection framework.....	8
b. Draft PDP Decree	8
4.3. Bundled consent.....	8
a. Existing data protection framework.....	8
b. Draft PDP Decree	8
c. Whether access to services may be conditional on consent	8
5. CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA	8
5.1. Existing data protection framework.....	8
5.2. Draft PDP Decree	9
5.3. Children.....	11
a. Existing data protection framework	11
b. Draft PDP Decree.....	11
5.4. Cookies, Internet of Things, online tracking.....	11
5.5. Direct marketing	11
a. Existing data protection framework	11
b. Draft PDP Decree.....	11
5.6. Biometric data	11
5.7. Genetic data	11
5.8. Financial information	11
5.9. Pseudonymized data	12
5.10. Location data	12
6. CONSENT FOR CROSS-BORDER DATA TRANSFERS.....	12
6.1. Existing data protection framework	12
6.2. Draft PDP Decree.....	12

7. TRANSPARENCY AND NOTICE	13
7.1. Existing data protection framework	13
7.2. Draft PDP Decree	13
8. SANCTIONS AND ENFORCEMENT	14
8.1. Existing data protection framework	14
a. Administrative sanctions	14
b. Criminal sanctions.....	14
c. Enforcement.....	15
8.2. Draft PDP Decree	15
a. Fines	15
b. Additional sanctions.....	16
c. Remedial measures.....	16
d. Compensation	16
9. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT SUBJECT TO A RISK IMPACT ASSESSMENT	16
10. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT IN OTHER CIRCUMSTANCES DEFINED BY LAW.....	17
10.1. Existing data protection framework	17
a. Network environments	17
b. Health sector	17
c. Credit sector.....	18
10.2. Draft PDP Decree.....	18
a. Processing of personal data without consent.....	18
b. Disclosure of personal data without consent.....	18
c. Sharing personal data with a third party, or granting a third party access to personal data.....	19
d. Scientific or statistical research.....	19

1. INTRODUCTION

Vietnam's existing data protection framework is highly fragmented. Vietnam does not currently have a comprehensive law regulating data protection and privacy, and instead, provisions on these issues (including several provisions on consent) are spread across various legal instruments.

To that end, in February 2021, Vietnam's Ministry of Public Security ("**MPS**") released for public consultation a draft omnibus data protection law, the Decree on Personal Data Protection ("**Draft PDP Decree**").¹

It is understood that following the public consultation, the MPS developed a revised Draft PDP Decree incorporating feedback from the public consultation. This revised draft has not been released to the public, and as of the date of this report, the Draft PDP Decree still has not been finalized or submitted to the government and National Assembly for final approval. However, it is expected that a finalized version of the Draft PDP Decree will be released in mid-2022.

Note: As the February 2021 version of the Draft PDP Decree is the only version that has been made public as of the date of this report, any reference to the "**Draft PDP Decree**" in this Report is to the draft released in February 2021 – please note that this version does not have legal effect and may be superseded.

The Draft PDP Decree seeks to introduce several major additions to Vietnam's personal data protection framework.

Firstly, the Draft PDP Decree seeks to establish a Personal Data Protection Committee ("**Committee**") under MPS' Department of Cybersecurity and High-Tech Crime Prevention and Control.² If the Draft PDP Decree is adopted in its current form, then the Committee's main responsibilities will be, among others, to enforce the PDP Decree and issue guidelines for compliance.³

Secondly, the Draft PDP Decree also seeks to introduce overarching principles that would govern the collection, processing, and sharing of personal data, namely:

- ▶ **Lawfulness:** Personal data shall only be collected where necessary in accordance with the law.⁴
- ▶ **Purpose limitation:** Personal data shall only be processed for specified purposes to which data subjects have consented or which have been registered.⁵
- ▶ **Data minimization:** Personal data may only be collected to the extent necessary to achieve the specified purpose(s).⁶
- ▶ **Restricted use:** Personal data may be used only with the consent of the data subject or with the permission of the public authority according to law.⁷
- ▶ **Data quality:** Personal data must be adequately updated to achieve processing purposes.⁸
- ▶ **Security:** Personal data must be subjected to protective measures throughout processing.⁹
- ▶ **Individuality:** Data subjects must be informed of all processing activities undertaken in relation to their personal data.¹⁰
- ▶ **Confidentiality:** Personal data must be kept confidential during processing.¹¹

¹ Available in Vietnamese at <http://bocongan.gov.vn/vanban/Pages/van-ban-moi.aspx?ItemID=418>

² Draft PDP Decree, Article 23(1).

³ See, generally, Draft PDP Decree, Articles 24 and 25.

⁴ Draft PDP Decree, Article 3(1).

⁵ Draft PDP Decree, Article 3(2).

⁶ Draft PDP Decree, Article 3(3).

⁷ Draft PDP Decree, Article 3(4).

⁸ Draft PDP Decree, Article 3(5).

⁹ Draft PDP Decree, Article 3(6).

¹⁰ Draft PDP Decree, Article 3(7).

¹¹ Draft PDP Decree, Article 3(8).

Thirdly, the Draft PDP Decree also seeks to provide data subjects with a number of rights over their personal data, namely, to:

- ▶ agree or disagree to the processing of their data by a “**personal data processor**”¹² or “**third party**”¹³ (subject to exceptions provided by law)¹⁴
- ▶ receive notice of processing from the personal data processor at the time of processing or as soon as practicable thereafter;¹⁵
- ▶ request that the personal data processor correct, view, or provide a copy of their personal data;¹⁶
- ▶ request that the personal data processor (subject to exceptions provided by law):
 - stop processing, disclosure, or provision of access to their personal data;
 - restrict access to their personal data;
 - delete their personal data;¹⁷
- ▶ complain to the Committee where:
 - their personal data has been infringed;¹⁸
 - their personal data has been processed for purposes other than those to which the data subject agrees or contrary to the provisions of law;¹⁹
 - their personal data rights have been violated or have not been properly exercised;²⁰ and
- ▶ claim compensation where there are grounds for believing that their personal data rights have been infringed.²¹

Lastly, the Draft PDP Decree seeks to impose general obligations on personal data processors to:

- ▶ restrict the ability of parties other than the data subject to access the data subject’s personal data under certain circumstances;²²
- ▶ ensure that personal data is accurate and complete;²³
- ▶ store legally processed personal data in an appropriate form and take measures to prevent illegal processing;²⁴
- ▶ cease processing, delete, and destroy the means of storing personal data where:
 - the personal data processor has failed to process the personal data for the registered purpose, or the purpose notified to the data subject;²⁵
 - storage of the personal data is no longer necessary for the personal data processor’s operations;²⁶

¹² Note that a “**personal data processor**” is defined as a domestic or foreign agency, organization, or individual that processes personal data (Draft PDP Decree, Article 2(8)).

¹³ Note that a “**third party**” is defined as a domestic and foreign agency, organization or individual that is entitled to receive personal data and have personal data processing activities but is not a personal data processor or data subject (Draft PDP Decree, Article 2(9)).

¹⁴ Draft PDP Decree, Article 5(1).

¹⁵ Draft PDP Decree, Article 5(2).

¹⁶ Draft PDP Decree, Article 5(3).

¹⁷ Draft PDP Decree, Article 5(4).

¹⁸ Draft PDP Decree, Article 5(5)(a).

¹⁹ Draft PDP Decree, Article 5(5)(b).

²⁰ Draft PDP Decree, Article 5(5)(c).

²¹ Draft PDP Decree, Article 5(6).

²² Draft PDP Decree, Article 7(1).

²³ Draft PDP Decree, Article 15.

²⁴ Draft PDP Decree, Article 16(1).

²⁵ Draft PDP Decree, Article 16(2)(a).

²⁶ Draft PDP Decree, Article 16(2)(b).

- Twenty years have passed since the death of the data subject, and the data subject has not made arrangements for continued processing of his/her data;²⁷ and
- ▶ when processing personal data, take measures to:
 - prevent unauthorized access to²⁸ and handling of²⁹ personal data, including during transfer, sharing, and transmission;³⁰
 - maintain detailed records on:
 - when, what, and from whom personal data was recorded, changed, or deleted or when personal data was accessed;³¹
 - transmission, sharing and transfer of personal data;³²
 - personal data processing equipment and software;³³ and
 - ensure that authorized persons can access and process personal data;³⁴
- ▶ establish a data protection department with a data protection officer to act as a point of contact for the Committee;³⁵ and
- ▶ establish procedures for receiving and responding to complaints in relation to personal data protection.³⁶

2. CONSENT AND PRIVACY SELF-MANAGEMENT IN EXISTING LAWS AND REGULATIONS

Under Vietnam's existing data protection framework, consent is generally the default requirement for collection, storage, use, processing, publication, disclosure, and transfer of information and materials related to an individual's private life or personal information of an individual, unless a relevant legal instrument provides an applicable exception.³⁷ Moreover, the law does not exclude reliance on consent in any specific circumstances (e.g., in an employment context, or if it is not feasible to obtain it).

Consent requirements ultimately derive from Article 21 of the 2013 Constitution, which provides, among other things, for the inviolability of personal privacy and legal protection of information regarding personal privacy and personal and familial secrecy.

These rights find expression in Vietnam's civil law primarily through Law No. 91/2015/QH13 ("**Civil Code**"),³⁸

Article 32 of the Civil Code provides individuals with a right over their own image. Subject to exceptions,³⁹ consent must be sought from individuals for use of their image.⁴⁰ If an individual's image is used for commercial purposes, then that individual has a right to remuneration, subject to any

²⁷ Draft PDP Decree, Article 16(2)(c).

²⁸ Draft PDP Decree, Article 17(2)(a).

²⁹ Draft PDP Decree, Article 17(2)(b).

³⁰ Draft PDP Decree, Article 17(2)(e).

³¹ Draft PDP Decree, Article 17(2)(c).

³² Draft PDP Decree, Article 17(2)(d).

³³ Draft PDP Decree, Article 17(2)(f).

³⁴ Draft PDP Decree, Article 17(2)(d).

³⁵ Draft PDP Decree, Article 18(2).

³⁶ Draft PDP Decree, Article 18(3).

³⁷ See, for example, Civil Code, Article 38; IT Law, Articles 21 and 22; Law on E-Transactions, Article 46; Law on Cyber Information Security, Article 17(1); Law on Consumer Protection, Articles 6(2)(b) and 6(2)(e); Decree No. 72, Article 21(7).

³⁸ The original text (in Vietnamese) is available on the National Law Database website at <http://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=9611>. An unofficial English translation is available at <https://wipolex-res.wipo.int/edocs/lexdocs/laws/en/vn/vn079en.pdf>.

³⁹ Civil Code, Article 32(2).

⁴⁰ Civil Code, Article 32(1).

agreement to the contrary.⁴¹ If an individual's image is used in violation of these provisions, then the individual has a right to request a court order compelling the violator or relevant entities to revoke, destroy, or terminate use of the image and provide compensation for any damage caused.⁴²

Additionally, Article 38 of the Civil Code expands on the constitutional right to privacy by requiring an individual's consent for collection, preservation, use, and publication of information about that individual's private life.⁴³ Subject to exceptions provided by law, consent of all family members is required for collection, preservation, use, and publication of information about family secrets.⁴⁴ Similar provisions can also be found in a wide variety of other legal instruments.⁴⁵

Additionally, various sectoral laws also provide for a measure of personal data protection within specialized domains, including:

cyberspace:

- ▶ Law No. 51/2005/QH11 on E-Transactions ("**Law on E-Transactions**");⁴⁶
- ▶ Law No. 67/2006/QH11 on Information Technology ("**IT Law**");⁴⁷
- ▶ Law No. 24/2018/QH14 on Cybersecurity ("**Law on Cybersecurity**");⁴⁸
- ▶ Law No. 86/2015/QH13 on Cyber Information Security ("**Law on Cyber Information Security**");⁴⁹
- ▶ Decree No. 91/2020/NĐ-CP on anti-spam ("**Decree No. 91**");⁵⁰
- ▶ Decree No. 72/2013/NĐ-CP on the management, provision, and use of internet services and online information,⁵¹ as amended and supplemented by Decree No. 27/2018/NĐ-CP⁵² ("**Decree No. 72**");
- ▶ Decree No. 15/2020/NĐ-CP providing penalties for administrative violations pertaining to postal, telecommunication, information technology, radio frequency areas and e-transactions ("**Decree No. 15**");⁵³

healthcare:

- ▶ Law No. 03/2007/QH12 on Prevention and Control of Infectious Diseases ("**Law on Prevention and Control of Infectious Disease**");⁵⁴

⁴¹ Civil Code, Article 32(1).

⁴² Civil Code, Article 32(3).

⁴³ Civil Code, Article 38(2).

⁴⁴ Civil Code, Article 38(2).

⁴⁵ See, for example, Law No. 10/2016/QH13 on Children ("**Law on Children**"), Article 6(11); Law on E-Transactions, Article 46(2); Law on Cybersecurity, Article 17.

⁴⁶ An English translation is available on the National Law Database website at <https://vbpl.vn/TW/Pages/vbpqen-toanvan.aspx?ItemID=6121>.

⁴⁷ An English translation is available on the National Law Database website at <http://vbpl.vn/TW/Pages/vbpqen-toanvan.aspx?ItemID=4773>.

⁴⁸ The original text (in Vietnamese) is available on the National Law Database website at <https://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=132957>. An unofficial English translation is available at <https://data.allens.com.au/pubs/pdf/priv/cupriv22jun18.pdf>.

⁴⁹ An English translation is available on the National Law Database website at <http://vbpl.vn/tw/Pages/vbpqen-toanvan.aspx?ItemID=11048>.

⁵⁰ The original text (in Vietnamese) is available on the National Law Database website at <https://vbpl.vn/TW/Pages/vbpq-van-ban-goc.aspx?ItemID=143897>. A summary in English is available at <https://www.lexology.com/library/detail.aspx?g=b1tedbb38-a6d5-45a5-9ccd-5e36a640de24>.

⁵¹ Available in Vietnamese on the National Law Database website at <http://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=30673>.

⁵² Available in Vietnamese on the National Law Database website at <http://vbpl.vn/TW/Pages/vbpq-van-ban-goc.aspx?ItemID=128671>.

⁵³ Available in Vietnamese on the National Law Database website at <https://vbpl.vn/TW/Pages/vbpq-van-ban-goc.aspx?ItemID=140561>.

⁵⁴ An English translation is available on the National Law Database website at <https://vbpl.vn/TW/Pages/vbpqen-toanvan.aspx?ItemID=3040>.

- ▶ Law No. 40/2009/QH12 on Medical Examination and Treatment (“**Law on Medical Examination and Treatment**”);⁵⁵

commerce:

- ▶ Law No. 59/2010/QH12 on Protection of Consumers' Rights (“**Law on Consumer Protection**”);⁵⁶
- ▶ Decree No. 52/2013/NĐ-CP on e-commerce,⁵⁷ as amended and supplemented by Decree No. 85/2021/NĐ-CP (“**Decree No. 52**”);⁵⁸

banking and finance:

- ▶ Law No. 47/2010/QH12 on Credit Institutions (“**Law on Credit Institutions**”);⁵⁹
- ▶ Decree No. 117/2018/NĐ-CP on protection of confidentiality and provision of client information of credit information and branches of foreign banks.⁶⁰

2.1. Health sector

The Law on Medical Examination and Treatment requires medical practices to maintain confidentiality over information relating to the health status and privacy of patients as indicated in their case history dossiers, except in limited circumstances.⁶¹ Accordingly, such information can generally only be disclosed with patients’ consent, subject to narrow exceptions as provided by law or for exchange of information and experience between practitioners, in order to improve the quality of diagnosis, care, and treatment.⁶²

2.2. Credit sector

The Law on Credit Institutions requires credit institutions and foreign bank branches to maintain confidentiality over information relating to their clients’ accounts, deposits, deposited assets, and transactions.⁶³ Credit institutions and foreign bank branches may not disclose such information to other organizations and individuals unless the client consents, or unless a competent state agency has made a request according to law.⁶⁴

3. CONSENT AND PRIVACY SELF-MANAGEMENT IN THE DRAFT PDP DECREE

Consent plays a prominent role in the Draft PDP Decree.

At the fundamental level, the Draft PDP Decree provides that data subjects have the right to agree or disagree to processing of their data by a personal data processor or third party (subject to exceptions provided by law).⁶⁵

⁵⁵ An English translation is available on the National Law Database website at <https://vbpl.vn/boyte/Pages/vbpqen-toanvan.aspx?ItemID=10482>.

⁵⁶ Note that in January 2022, Vietnam’s Ministry of Industry and Trade (“**MOIT**”) released a draft revised Law on Consumer Protection, which aims to supersede the existing Law on Consumer Protection enacted in 2010.

⁵⁷ The original text (in Vietnamese) is available on the National Law Database website at <http://vbpl.vn/bocongthuong/Pages/vbpq-toanvan.aspx?ItemID=30470>.

⁵⁸ Available in Vietnamese on the National Law Database website at <https://vbpl.vn/TW/Pages/vbpq-van-ban-goc.aspx?ItemID=150735>.

⁵⁹ Available in Vietnamese on the National Law Database website at <https://vbpl.vn/nganhngnhanuoc/pages/vbpq-luocdo.aspx?ItemID=25693>.

⁶⁰ Available in Vietnamese on the National Law Database website at <https://vbpl.vn/nganhngnhanuoc/Pages/vbpq-toanvan.aspx?ItemID=130985>.

⁶¹ Law on Medical Examination and Treatment, Article 3(2).

⁶² Law on Medical Examination and Treatment, Article 8(2).

⁶³ Law on Credit Institutions, Article 14(2).

⁶⁴ Law on Credit Institutions, Article 14(3).

⁶⁵ Draft PDP Decree, Article 5(1).

The Draft PDP Decree permits processing⁶⁶ or disclosure of a data subject's personal data if:

- ▶ a personal data processor or third party has obtained the data subject's consent;⁶⁷ or
- ▶ an alternative legal basis for processing⁶⁸ or disclosing⁶⁹ personal data without consent applies.

Accordingly, the default rule under the Draft PDP Decree appears to be that unless an alternative legal basis exists, or an exception applies, the consent of a data subject is required to:

- ▶ use the data subject's personal data;⁷⁰
- ▶ process the data subject's personal data;⁷¹
- ▶ disclose the data subject's personal data;⁷²
- ▶ share data subject's personal data with a third party;⁷³ and
- ▶ grant a third party access to the data subject's personal data.⁷⁴

Additionally, consent of the data subject is one of a number of requirements for transfer of the data subject's personal data out of Vietnam.⁷⁵

4. CONDITIONS FOR CONSENT

4.1. Definition and forms of consent

Generally, under prevailing laws, consent must be freely given. Prevailing laws generally do not require consent to be given in any specific form, except in the contexts of e-commerce platforms and advertising or marketing communications, which are subject to more stringent requirements (see below). It is also currently unclear whether prevailing laws would recognize implied consent as valid consent.

a. Consent in e-commerce

Decree No. 52 requires an e-commerce platforms to develop a mechanism for its customers to provide consent explicitly through an online function on the platform (e.g., a click-to-accept mechanism), emails, messages, or otherwise as agreed upon by the platform and its users.⁷⁶

Further, if customers' personal data will be used for marketing purposes or will be shared with, disclosed, or transferred to third parties,⁷⁷ the customers' consent must be expressly obtained through a separate mechanism that enables the customers to decide whether to permit use of their personal data for such purposes.

For example, the e-commerce platform may provide customers with a tick box to choose whether to permit the e-commerce platform to use their personal information for marketing purposes or disclose it to, or share it with, third parties.

⁶⁶ Note that “**processing of personal data**” is defined to include collection, recording, analysis, storage, change, disclosure, granting of access, retrieval, collection, recovery, encryption, decryption, copying, transfer, deletion, and destruction of personal data, as well as other related actions (Draft PDP Decree, Article 2(6)).

⁶⁷ Draft PDP Decree, Article 3(4).

⁶⁸ See Draft PDP Decree, Article 10(1).

⁶⁹ See Draft PDP Decree, Articles 6(1) and 10(2).

⁷⁰ Draft PDP Decree, Article 3(4).

⁷¹ Draft PDP Decree, Article 10(1).

⁷² Draft PDP Decree, Article 6(1).

⁷³ Draft PDP Decree, Article 10(2).

⁷⁴ Draft PDP Decree, Article 10(2).

⁷⁵ Draft PDP Decree, Article 21(1)(a) and 21(3)(a).

⁷⁶ Decree No. 52, Article 70.

⁷⁷ Decree No. 52, Article 70(3).

b. Consent to receive advertising or marketing communications

Decree No. 91 prohibits organizations and individuals from sending advertising or marketing communications to individuals unless the individuals have expressly “opted in” to receive such communication by:

- ▶ agreeing to receive advertising text messages after the advertiser sends the first and only message requesting that users register to receive advertising messages from the advertiser;⁷⁸
- ▶ completing a form and making a confirmation on paper or on the website/web portal, online application, or social network of the advertiser;⁷⁹
- ▶ calling or sending a message to the advertiser’s call center to subscribe;⁸⁰ or
- ▶ using a software program to subscribe.⁸¹

c. Consent in the Draft PDP Decree

Under the Draft PDP Decree, consent is only valid if given voluntarily⁸² and with knowledge of:

- ▶ the type of data to be processed;⁸³
- ▶ the purpose for processing;⁸⁴
- ▶ the parties permitted to process and share the data;⁸⁵
- ▶ the conditions for transferring and sharing the data to third parties;⁸⁶ and
- ▶ the rights of data subjects in relation to the processing of their personal data according to law.⁸⁷

Consent must also be given in a format that can be printed and reproduced in writing⁸⁸ and cannot be inferred from silence or non-response of data subjects.⁸⁹

Consent for processing of sensitive personal data must be given in a printable format and copied in text.⁹⁰ When obtaining consent for such processing, the personal data processor must also explain to the data subject that the personal data to be processed is sensitive personal data.⁹¹

Note that the Draft PDP Decree recognizes a form of deemed consent in the narrow context of audio or video recording activities in public places by competent state agencies, where prescribed by law.⁹²

By default, the collecting agency must notify data subjects of the recording in a way that data subjects understand.⁹³ However, this requirement does not apply where recording is for the purposes of national defense, security, social order and safety, social ethics, or the health of the community.⁹⁴

⁷⁸ Decree No. 91, Article 13(2)(a).

⁷⁹ Decree No. 91, Article 13(2)(b).

⁸⁰ Decree No. 91, Article 13(2)(c).

⁸¹ Decree No. 91, Article 13(2)(d).

⁸² Draft PDP Decree, Article 8(1).

⁸³ Draft PDP Decree, Article 8(2)(a).

⁸⁴ Draft PDP Decree, Article 8(2)(b).

⁸⁵ Draft PDP Decree, Article 8(2)(c).

⁸⁶ Draft PDP Decree, Article 8(2)(d).

⁸⁷ Draft PDP Decree, Article 8(2)(đ).

⁸⁸ Draft PDP Decree, Article 8(4).

⁸⁹ Draft PDP Decree, Article 8(3).

⁹⁰ Draft PDP Decree, Article 8(5).

⁹¹ Draft PDP Decree, Article 8(5).

⁹² Draft PDP Decree, Article 6(4).

⁹³ Draft PDP Decree, Article 6(4)(a).

⁹⁴ Draft PDP Decree, Article 6(4)(b).

4.2. Withdrawal of consent

a. Existing data protection framework

Vietnamese law allows the consent to be withdrawn by the data subject at any time. If the data subject withdraws consent to processing of his/her personal data, the data processor would no longer be entitled to process and/or share such data.

b. Draft PDP Decree

The Draft PDP Decree expressly provides that consent can be withdrawn at any time.⁹⁵

The Draft PDP Decree further provides data subjects with a right to request that a personal data processor stop processing or disclosing personal data, except where processing or disclosure is required by law.⁹⁶

If a personal data processor continues to process personal data after the data subject has withdrawn consent and/or sent a request to stop processing or disclosure of his/her personal data, then the processor could face an administrative fine, a requirement to pay compensation, suspension of its ability to process personal data for 1 to 3 months, and withdrawal of the Committee's approval to process sensitive personal data and/or transfer personal data out of Vietnam.⁹⁷

4.3. Bundled consent

a. Existing data protection framework

In general, bundled consent is acceptable in Vietnam as prevailing laws do not specifically prohibit this practice. An exception to this is that pursuant to Decree No. 52 (see above), which applies to e-commerce platforms, consent for marketing and sharing purposes must be obtained separately from consent for other activities.⁹⁸

b. Draft PDP Decree

The Draft PDP Decree does not expressly provide for bundled consent. It is therefore possible that if the Draft PDP Decree is enacted, a personal data processor could rely on bundled consent, provided that other requirements under the Draft PDP Decree and other prevailing laws (such as Decree No. 52) are met (see above). However, note that in the event of a dispute, the personal data processor bears the burden of proving that consent has been obtained.⁹⁹

c. Whether access to services may be conditional on consent

Neither prevailing laws nor the Draft PDP Decree provide for this. It is therefore possible that provision of services could be made conditional on the data subject consenting to processing of his/her personal data.

5. CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA

5.1. Existing data protection framework

Strictly speaking, prevailing laws do not distinguish between different classes of personal data. However, due to the fragmented nature of Vietnam's data protection landscape, personal information collected and used in a given sector (e.g., healthcare, finance) may be subject to sector-specific requirements in sectoral laws and regulations.

⁹⁵ Draft PDP Decree, Article 8(7).

⁹⁶ Draft PDP Decree, Article 5(4).

⁹⁷ See, generally, Draft PDP Decree, Article 22.

⁹⁸ Decree No. 52, Article 70(3).

⁹⁹ Draft PDP Decree, Article 8(8).

5.2. Draft PDP Decree

The Draft PDP Decree distinguishes between “basic personal data”¹⁰⁰ and “sensitive personal data.”¹⁰¹

Basic personal data includes a person’s:

- ▶ full name, middle name, birth name, or alias (if any);¹⁰²
- ▶ date of birth, death, or having gone missing;¹⁰³
- ▶ blood group;¹⁰⁴
- ▶ sex;¹⁰⁵
- ▶ place of birth;¹⁰⁶
- ▶ place of current or permanent residence;¹⁰⁷
- ▶ hometown;¹⁰⁸
- ▶ contact address;¹⁰⁹
- ▶ email address;¹¹⁰
- ▶ education level;¹¹¹
- ▶ ethnicity;¹¹²
- ▶ nationality;¹¹³
- ▶ telephone number;¹¹⁴
- ▶ Identity card number, passport number, citizen identification number, driving license number, license plate number, personal tax identification number, and social insurance number;¹¹⁵
- ▶ marital status;¹¹⁶ and
- ▶ data that reflects activity or history of activity in cyberspace.¹¹⁷

Sensitive personal data includes:

- ▶ personal data on political and religious views;¹¹⁸
- ▶ personal health data, i.e., information relating to the physical or mental health status of the data subject that has been collected and identified during the process of registration or provision of medical services;¹¹⁹

¹⁰⁰ Draft PDP Decree, Article 2(2).

¹⁰¹ Draft PDP Decree, Article 2(3).

¹⁰² Draft PDP Decree, Article 2(2)(a).

¹⁰³ Draft PDP Decree, Article 2(2)(b).

¹⁰⁴ Draft PDP Decree, Article 2(2)(c).

¹⁰⁵ Draft PDP Decree, Article 2(2)(c).

¹⁰⁶ Draft PDP Decree, Article 2(2)(d).

¹⁰⁷ Draft PDP Decree, Article 2(2)(d).

¹⁰⁸ Draft PDP Decree, Article 2(2)(d).

¹⁰⁹ Draft PDP Decree, Article 2(2)(d).

¹¹⁰ Draft PDP Decree, Article 2(2)(d).

¹¹¹ Draft PDP Decree, Article 2(2)(d).

¹¹² Draft PDP Decree, Article 2(2)(e).

¹¹³ Draft PDP Decree, Article 2(2)(g).

¹¹⁴ Draft PDP Decree, Article 2(2)(h).

¹¹⁵ Draft PDP Decree, Article 2(2)(i).

¹¹⁶ Draft PDP Decree, Article 2(2)(j).

¹¹⁷ Draft PDP Decree, Article 2(2)(k).

¹¹⁸ Draft PDP Decree, Article 2(3)(a).

¹¹⁹ Draft PDP Decree, Article 2(3)(b).

- ▶ personal genetic data, i.e., information relating to inherited or acquired genetic characteristics of an individual;¹²⁰
- ▶ personal biometric data, i.e., information about physical and biological characteristics of an individual;¹²¹
- ▶ personal data on gender status, i.e., information about people identified as male, female, gender neutral, androgynous, having both masculine and feminine characteristics, or self-identifying as a different gender from the gender identified at birth;¹²²
- ▶ personal data about life and sexual orientation;¹²³
- ▶ personal data about criminals and criminal acts collected and stored by law enforcement agencies;¹²⁴
- ▶ personal financial data, i.e., information used to identify an account, card or payment instrument provided by a financial institution to a data subject or information about the relationship between a financial institution and a data subject;¹²⁵
- ▶ personal location data, i.e., information about the individual's physical location in the past or present;¹²⁶
- ▶ personal data about social relationships;¹²⁷
- ▶ other personal data as specified by law to be special and subject to confidentiality protection.¹²⁸

Notably, entities seeking to process sensitive personal data must register with the Committee before processing such data,¹²⁹ except where processing is for the purpose(s) of:

- ▶ preventing, detecting, investigating, and handling illegal acts;¹³⁰
- ▶ performing state agencies' healthcare functions in accordance with law;¹³¹
- ▶ serving the judicial functions of Court;¹³²
- ▶ research, archiving, or statistical analysis by a state agency or scientific research organization which have been certified by the Committee;¹³³
- ▶ other activities prescribed by law.¹³⁴

The entity wishing to collect and/or process sensitive personal data must prepare and submit an impact assessment report addressing the potential harm to data subjects regarding the proposed processing and measures to manage, minimize, or eliminate such harm.

¹²⁰ Draft PDP Decree, Article 2(3)(c).

¹²¹ Draft PDP Decree, Article 2(3)(d).

¹²² Draft PDP Decree, Article 2(3)(đ).

¹²³ Draft PDP Decree, Article 2(3)(e).

¹²⁴ Draft PDP Decree, Article 2(3)(f).

¹²⁵ Draft PDP Decree, Article 2(3)(g).

¹²⁶ Draft PDP Decree, Article 2(3)(h).

¹²⁷ Draft PDP Decree, Article 2(3)(i).

¹²⁸ Draft PDP Decree, Article 2(3)(j).

¹²⁹ Draft PDP Decree, Article 20(1).

¹³⁰ Draft PDP Decree, Article 20(4)(a).

¹³¹ Draft PDP Decree, Article 20(4)(b).

¹³² Draft PDP Decree, Article 20(4)(c).

¹³³ Draft PDP Decree, Article 20(4)(d).

¹³⁴ Draft PDP Decree, Article 20(4)(đ).

5.3. Children

a. Existing data protection framework

The Law on Children prohibits announcing or disclosing information on the personal life or secrets of a child who has reached the age of 7 years without first obtaining the consent of both the child and his/her parents or guardians.¹³⁵

b. Draft PDP Decree

Before processing a child's data, a personal data processor must verify the child's age and obtain the consent of the child's parent or guardian.¹³⁶ The child's parent or guardian may also withdraw consent to processing of the child's personal data, in which case, such processing must cease.¹³⁷

These provisions are subject to the proviso that processing of children's personal data must always be done in accordance with the principle of protecting children's rights and in the children's best interests.¹³⁸

5.4. Cookies, Internet of Things, online tracking

The Draft PDP Decree does not specifically provide for cookies, the Internet of Things, or online tracking. However, note that data which reflects a person's activity or history of activity in cyberspace qualifies as "basic personal data" and not "sensitive personal data" under the Draft PDP Decree.¹³⁹

5.5. Direct marketing

a. Existing data protection framework

As discussed above, the general rule under Vietnamese law is that a recipient of advertising or marketing communication must consent in a prescribed manner to receive such communication. Additionally, an e-commerce platform must provide a separate mechanism for obtaining consent to use customers' information for marketing purposes.

b. Draft PDP Decree

The Draft PDP Decree does not make specific provision for direct marketing.

5.6. Biometric data

Personal biometric data – defined as information about the physical attributes and biological characteristics of an individual – qualifies as sensitive personal data under the Draft PDP Decree.¹⁴⁰

5.7. Genetic data

Personal genetic personal data – defined as information relating to inherited or acquired genetic characteristics of an individual – qualifies as sensitive personal data under the Draft PDP Decree.¹⁴¹

5.8. Financial information

Personal financial information – defined as information used to identify accounts, cards, or payment instruments provided by financial institutions to data subjects, or information about the relationship

¹³⁵ Law on Children, Article 6(11).

¹³⁶ Draft PDP Decree, Article 14(1)(b).

¹³⁷ Draft PDP Decree, Article 14(4)(b).

¹³⁸ Draft PDP Decree, Article 14(1)(a).

¹³⁹ Draft PDP Decree, Article 2(2)(l).

¹⁴⁰ Draft PDP Decree, Article 2(3)(d).

¹⁴¹ Draft PDP Decree, Article 2(3)(c).

between financial institutions and data subjects – qualifies as sensitive personal data under the Draft PDP Decree.¹⁴²

5.9. Pseudonymized data

The Draft PDP Decree does not make specific provisions for pseudonymized personal data but does permit use of pseudonymized data without data subjects' consent for scientific or statistical research purposes, under certain circumstances (see below).¹⁴³ Notably, this legal basis is only available to personal data processors which, among other requirements, have registered with the Committee to process sensitive personal data.¹⁴⁴

5.10. Location data

Personal location data – defined as information about an individual's physical location in the past or present – qualifies as sensitive personal data under the Draft PDP Decree.¹⁴⁵

6. CONSENT FOR CROSS-BORDER DATA TRANSFERS

6.1. Existing data protection framework

Under prevailing laws, there are few specific requirements governing cross-border transfer of personal data out of Vietnam. Provided that the data controller obtains prior consent from the data subject,¹⁴⁶ the data controller would likely be able to transfer such personal information to other entities outside of Vietnam.

6.2. Draft PDP Decree

Under the Draft PDP Decree, consent is one of several cumulative conditions for transferring personal data of Vietnamese citizens out of Vietnam's territorial borders.¹⁴⁷

The other conditions are that the Committee consents in writing to the transfer,¹⁴⁸ that the original data is stored in Vietnam,¹⁴⁹ and that there is a document proving that the laws of the destination jurisdiction protect personal data to an equal or greater level than that specified in the Draft PDP Decree.¹⁵⁰

Consent of the data subject *may* also function as an exception,¹⁵¹ though this is unclear as exception does not specify whether such consent *alone* would be sufficient, or whether the other circumstances referred to in the exception function as *additional conditions* which would have to be met. These circumstances include:

- ▶ the written consent of the Committee to the transfer;¹⁵²
- ▶ a commitment given by the recipient to protect the personal data to be transferred;¹⁵³
- ▶ a commitment given by the recipient to apply the personal data protection measures employed by the personal data processor.¹⁵⁴

¹⁴² Draft PDP Decree, Article 2(3)(h).

¹⁴³ See, generally, Draft PDP Decree, Article 12.

¹⁴⁴ Draft PDP Decree, Article 12(4)(d).

¹⁴⁵ Draft PDP Decree, Article 2(3)(i).

¹⁴⁶ Law on Cyber Information Security, Article 17(1)(c).

¹⁴⁷ Draft PDP Decree, Article 21(1)(a).

¹⁴⁸ Draft PDP Decree, Article 21(1)(d).

¹⁴⁹ Draft PDP Decree, Article 21(1)(b).

¹⁵⁰ Draft PDP Decree, Article 21(1)(c).

¹⁵¹ Draft PDP Decree, Article 21(3)(a).

¹⁵² Draft PDP Decree, Article 21(3)(b).

¹⁵³ Draft PDP Decree, Article 21(3)(c).

¹⁵⁴ Draft PDP Decree, Article 21(3)(d).

The Draft PDP Decree requires the Committee, in determining whether to approve the transfer, to have regard to whether:

- ▶ the data subjects' rights under the Draft PDP Decree will be effectively protected in the destination jurisdiction;¹⁵⁵
- ▶ the personal data processor has committed to register to transfer personal data across borders;¹⁵⁶ and
- ▶ the personal data processor has indicated the measures that will be employed to protect the personal data.¹⁵⁷

A personal data processor that transfers personal data across borders is required to build a system for retaining data transfer history for a period of 3 years.¹⁵⁸ This system is subject to annual evaluation by the Committee.¹⁵⁹

7. TRANSPARENCY AND NOTICE

7.1. Existing data protection framework

Under prevailing laws, an organization or individual that handles personal data must inform the data subject of the scope and purpose for collection and use of the data before obtaining consent.¹⁶⁰

7.2. Draft PDP Decree

As discussed above, consent is only valid under the Draft PDP Decree if the data subject has been informed of the following:

- ▶ the type of data to be processed;¹⁶¹
- ▶ the purpose for processing;¹⁶²
- ▶ the parties permitted to process and share the data;¹⁶³
- ▶ the conditions for transferring and sharing the data to third parties;¹⁶⁴ and
- ▶ the rights of data subjects in relation to the processing of their personal data according to law.¹⁶⁵

Further, consent to processing of sensitive personal data is only valid if the personal data processor has explained to the data subject that the data to be processed is sensitive personal data, and the data subject has given consent in writing.¹⁶⁶

The Draft PDP Decree also provides data subjects with the right to receive notice of processing from the personal data processor at the time of processing or as soon as practicable thereafter.¹⁶⁷ Accordingly, the data subject also must be notified of all personal data processing activities,¹⁶⁸ except where:

¹⁵⁵ Draft PDP Decree, Article 21(2)(a).

¹⁵⁶ Draft PDP Decree, Article 21(2)(b).

¹⁵⁷ Draft PDP Decree, Article 21(2)(c).

¹⁵⁸ Draft PDP Decree, Article 21(4).

¹⁵⁹ Draft PDP Decree, Article 21(5).

¹⁶⁰ Law on Cyber Information Security, Article 17(1)(a); IT Law, Article 21(1)(a); Law on Consumer Protection, Articles 6(2)(a) and 6(2)(b).

¹⁶¹ Draft PDP Decree, Article 8(2)(a).

¹⁶² Draft PDP Decree, Article 8(2)(b).

¹⁶³ Draft PDP Decree, Article 8(2)(c).

¹⁶⁴ Draft PDP Decree, Article 8(2)(d).

¹⁶⁵ Draft PDP Decree, Article 8(2)(đ).

¹⁶⁶ Draft PDP Decree, Article 8(5).

¹⁶⁷ Draft PDP Decree, Article 5(2).

¹⁶⁸ Draft PDP Decree, Article 11(1). Note that Article 11(2) of the Draft PDP Decree specifies the information that must be provided in the notification.

- ▶ the data subject has fully consented to the content and processing of personal data;¹⁶⁹
- ▶ the processing is regulated by law or an international agreement or treaty;¹⁷⁰
- ▶ the processing does not affect the rights and interests of the data subject, and it is not possible to notify the data subject;¹⁷¹ or
- ▶ the processing is for scientific or statistical research according to Article 12 of the Draft PDP Decree.¹⁷²

8. SANCTIONS AND ENFORCEMENT

8.1. Existing data protection framework

Breach of consent requirements may give rise to administrative or criminal sanctions, depending on the scale of the breach.

a. Administrative sanctions

Penalties for the breach of consent requirements are present in a number of different legal instruments.

For example, under “**Decree No. 98/2020/NĐ-CP prescribing penalties on administrative violations against regulations on commerce, production and trade in counterfeit and prohibited goods, and protection of consumer rights**,”¹⁷³ a person who breaches certain consent requirements faces a penalty of between VND 10 million and VND 40 million, depending on the nature of the breach. Further, an e-commerce platform that breaches such requirements on multiple consecutive occasions might be asked to suspend operation of its platform for a period of 6-12 months. In both cases, the infringing party must also remit any money obtained from the breach of the relevant consent requirements to the competent authority.

Under “**Decree No. 15/2020/NĐ-CP prescribing penalties for administrative violations against regulations on postal services, telecommunications, radio frequencies, information technology and electronic transactions**,”¹⁷⁴ a person who breaches certain consent requirements faces a penalty of between VND 10 million and VND 30 million, depending on the nature of the breach. If the infringing party is an organization, the monetary sanction is doubled.

b. Criminal sanctions

Under Law No. 100/2015/QH13 (the “**Penal Code**”),¹⁷⁵ the offender may also be subject to a warning, a fine of up to VND 50 million, or a community sentence of up to 3 years for an act that infringes upon secret information, mail, telephone, or telegraph privacy or other means of private information exchange.¹⁷⁶

If any of the following circumstances applies, then the offender also faces 1 to 3 years’ imprisonment:

- ▶ the offense is committed by an organized group;
- ▶ the offense involves abuse of the offender’s position or power;
- ▶ the offense has been committed more than once;
- ▶ the information obtained is disclosed and affects another person’s dignity or reputation; or

¹⁶⁹ Draft PDP Decree, Article 11(3)(a).

¹⁷⁰ Draft PDP Decree, Article 11(3)(b).

¹⁷¹ Draft PDP Decree, Article 11(3)(c).

¹⁷² Draft PDP Decree, Article 11(3)(d).

¹⁷³ Available in Vietnamese on the National Law Database website at <https://vbpl.vn/bocongthuong/Pages/vbpq-luocdo.aspx?ItemID=143881>.

¹⁷⁴ Available in Vietnamese on the National Law Database website at <https://vbpl.vn/tw/Pages/vbpq-van-ban-goc.aspx?dvid=13&ItemID=140561>.

¹⁷⁵ Available in Vietnamese on the National Law Database website at <https://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=96122>.

¹⁷⁶ Penal Code, Article 159(1).

- ▶ the offense results in the suicide of the victim.¹⁷⁷

An offender faces a fine of up to VND 200 million, a community sentence of up to 3 years, or 3 to 36 months' imprisonment, if the offender:

- ▶ earns an illegal profit in the sum of VND 50 million to VND 200 million,
- ▶ causes property damage assessed at between VND 100 million and VND 500 million; or
- ▶ damages the reputation of an organization or individual by:
 - uploading information on a computer or telecommunications network in violation of regulations or law;
 - trading, exchanging, giving, changing, or publishing private information of an organization or individual on the computer or telecommunications network without the consent of the information owner;
- ▶ engages in other acts that involve illegal use of information on the computer or telecommunications network.¹⁷⁸

The penalty increases to a fine of between VND 200 million and VND 1 billion or to 2 to 7 years' imprisonment if any of the foregoing offenses is committed in any of the following circumstances:

- ▶ the offense is committed by an organized group;
- ▶ the offender misuses his/her position as the administrator of the computer or telecommunications network;
- ▶ the illegal profit earned exceeds VND 200 million;
- ▶ the property damage caused by the offense is assessed to exceed VND 500 million;
- ▶ the offense involves infringement of privacy which results in the suicide of the victim;
- ▶ the offense has a negative impact on social security, order or safety or Vietnam's diplomatic relationships; or
- ▶ the offense results in a demonstration.¹⁷⁹

c. Enforcement

To date, there have been too few cases in Vietnam to give an indication of whether notice and consent requirements are effectively enforced.

However, a highly publicized criminal case in 2017 involved breach of consent requirements using malicious software. In this case, the infringer, Huynh Ngoc Den, supplied customers with a software application named COPYPHONE which could be installed on another person's smartphone to record messages, call-logs, etc. without the person's consent. The People's Court of Ho Chi Minh City sentenced Huynh Ngoc Den to four years in prison for the offense of "illegal access to computer networks, telecommunications networks, the Internet, or digital devices of other people."

8.2. Draft PDP Decree

a. Fines

A fine of VND 50 to 80 million or up to 5% of the violating personal data processor's revenue in Vietnam might be applied for a first-time violation of, among others, the Draft PDP Decree's consent requirements.¹⁸⁰

¹⁷⁷ Penal Code, Article 159(2).

¹⁷⁸ Penal Code, Article 288(1).

¹⁷⁹ Penal Code, Article 288(2).

¹⁸⁰ Draft PDP Decree, Article 22.1(a)-(m).

The possible fine increases to VND 80 million to VND 100 million for a second-time violation¹⁸¹ and 5% of the violating personal data processor's revenue in Vietnam for a third-time violation.¹⁸²

b. Additional sanctions

The Draft PDP Decree also provides for additional sanctions in the forms of:

- ▶ suspension of personal data processing for 1-3 months for a second-time violation;¹⁸³ and
- ▶ withdrawal of the Committee's approval to processing of sensitive personal data and/or transferring of personal data out of Vietnam's territorial borders.¹⁸⁴

c. Remedial measures

The Draft PDP Decree empowers the Committee to order an entity which has committed a violation to repay any money obtained from the violation.¹⁸⁵

d. Compensation

Regarding processing of personal data, data subjects have the right, among others, to claim compensation where there are grounds for believing that their personal data rights have been infringed.¹⁸⁶

9. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT SUBJECT TO A RISK IMPACT ASSESSMENT

Vietnam's existing data protection framework does not provide for a balancing test for processing personal data without consent, such as that envisaged under the "legitimate interests" basis under the EU GDPR.

The February 2021 version of the Draft PDP Decree also does not provide for such a basis. However, the Draft PDP Decree appears to contain an implicit requirement for a personal data processor to conduct a balancing test before disclosing sensitive personal data (irrespective of the legal basis relied upon for such disclosure). Specifically, Article 6(3) of the Draft PDP Decree prohibits disclosure of personal data to a third party where such disclosure would harm the legitimate interests of the data subject. To comply with this provision, a personal data processor who intends to disclose sensitive personal data would necessarily have to consider what the data subject's legitimate interests are, and whether the disclosure would harm such interests.

This is not as comprehensive as the balancing test under the GDPR, which requires a data controller to specify a legitimate interest of the data controller or a third party and consider, firstly, whether processing is necessary for pursuit of that legitimate interest, and secondly, whether the rights and freedoms of the data subject override the legitimate interest relied upon.

However, the test in the Draft PDP Decree shares certain elements with the GDPR's test in that both would minimally require consideration of the impact of disclosure for a particular purpose on the data subject.

¹⁸¹ Draft PDP Decree, Article 22(2)(d).

¹⁸² Draft PDP Decree, Article 22(3)(a).

¹⁸³ Draft PDP Decree, Article 22(4)(a).

¹⁸⁴ Draft PDP Decree, Article 22(4)(b).

¹⁸⁵ Draft PDP Decree, Article 22(5).

¹⁸⁶ Draft PDP Decree, Article 5(6).

10. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT IN OTHER CIRCUMSTANCES DEFINED BY LAW

10.1. Existing data protection framework

a. Network environments

The IT Law permits organizations and individuals that collect, process, and use personal information in a network environment to do so without the data subjects' consent for the following purposes:

- ▶ signing, modifying, or performing contracts on the use of information, products, or services in the network environment;¹⁸⁷
- ▶ calculating charges for use of information, products, or services in the network environment;¹⁸⁸ and
- ▶ performing other obligations provided for by law.¹⁸⁹

Organizations and enterprises that provide online services may disclose personal information of service users without such users' consent:

- ▶ where such organizations and enterprises reach written agreements on the provision of personal information to calculate charges, make invoices and documents, and prevent evasion of contractual obligations;¹⁹⁰ or
- ▶ at the request of competent state management agencies as prescribed by law.¹⁹¹

b. Health sector

In the health sector, the Law on Medical Examination and Treatment provides exceptions to consent requirements for disclosure of information in patients' case history dossiers.

Firstly, information on patients' health status and other private information in such dossiers may be disclosed without patients' consent where the disclosure is for the purpose of exchange of information and experience between practitioners who directly treat the patients to improve the quality of diagnosis, care, and treatment, or in other cases provided by law.¹⁹²

Secondly, certain parties are permitted to access these dossiers without patients' consent for on-the-spot-reading or for copying for certain purposes. These include:

- ▶ for research or professional purposes,
 - trainee students, researchers, and
 - practitioners of medical examination and treatment establishments;¹⁹³ and
- ▶ for performance of their assigned tasks according to their vested powers,
 - representatives of state health management agencies that directly manage medical examination and treatment establishments;
 - investigative agencies;
 - procuracies;
 - courts;

¹⁸⁷ IT Law, Article 21(3)(a).

¹⁸⁸ IT Law, Article 21(3)(b).

¹⁸⁹ IT Law, Article 21(3)(c).

¹⁹⁰ Decree No. 72, Article 21(7)(b).

¹⁹¹ Decree No. 72, Article 21(7)(c).

¹⁹² Law on Medical Treatment, Article 8(2).

¹⁹³ Law on Medical Treatment, Article 59(4)(a).

- health inspectors;
- insurance agencies;
- forensic and mental forensic examination organizations; and
- lawyers.¹⁹⁴

c. Credit sector

The Law on Credit Institutions requires credit institutions and foreign bank branches to maintain confidentiality over information relating to their clients' accounts, deposits, deposited assets, and transactions.¹⁹⁵ However, credit institutions and foreign bank branches may disclose such information to other organizations and individuals without a client's consent where a competent state agency has made a request according to law.¹⁹⁶

10.2. Draft PDP Decree

a. Processing of personal data without consent

The Draft PDP Decree permits personal data processors to *process* personal data without the data subject's consent where the processing is:

- ▶ according to the provisions of law;¹⁹⁷
- ▶ in the interests of national security, social order, and safety;¹⁹⁸
- ▶ required by law in emergency events that threaten the life, or seriously affect the health of, the data subject or the public health;¹⁹⁹
- ▶ in support of investigation and handling of regulatory violations;²⁰⁰
- ▶ in compliance with specific provisions of international agreements or treaties to which Vietnam is a signatory that explicitly allow the processing of personal data without the data subject's consent;²⁰¹ or
- ▶ In respect of de-identified personal data for research or statistics purposes, in compliance with the requirements in Article 12 of the Draft PDP Decree.²⁰²

b. Disclosure of personal data without consent

Personal data processors and third parties may *disclose* personal data without the data subject's consent where disclosure is:

- ▶ according to the provisions of law;²⁰³
- ▶ necessary for the interests of national security, social order, and safety;²⁰⁴
- ▶ made in the media:
 - for the purposes of national defense and security, social order and safety, social ethics, and community health;²⁰⁵ or

¹⁹⁴ Law on Medical Treatment, Article 59(4)(b).

¹⁹⁵ Law on Credit Institutions, Article 14(2).

¹⁹⁶ Law on Credit Institutions, Article 14(3).

¹⁹⁷ Draft PDP Decree, Article 10(1)(a).

¹⁹⁸ Draft PDP Decree, Article 10(1)(b).

¹⁹⁹ Draft PDP Decree, Article 10(1)(c).

²⁰⁰ Draft PDP Decree, Article 10(1)(d).

²⁰¹ Draft PDP Decree, Article 10(1)(d).

²⁰² Draft PDP Decree, Articles 10(1)(e) and 12.

²⁰³ Draft PDP Decree, Article 6(1)(a)

²⁰⁴ Draft PDP Decree, Article 6(1)(b).

²⁰⁵ Draft PDP Decree, Article 6(1)(c).

- according to the provisions of the Press Law in a manner that does not cause economic, reputational, psychological, or material damage to the data subject;²⁰⁶ or
- ▶ as required by law in emergency events that threaten the life, or seriously affect the health of, the data subject or the public health.²⁰⁷

c. Sharing personal data with a third party, or granting a third party access to personal data

Personal data processors may *share personal data with a third party* or *grant a third party access to personal data* without the data subject's consent where sharing or granting access:

- ▶ is according to the provisions of law or international agreements or treaties to which Vietnam is a signatory;²⁰⁸
- ▶ is to protect the life, health, or freedom of the data subject;²⁰⁹
- ▶ does not affect the rights and interests of the data subject, and it is impossible to obtain the data subject's consent;²¹⁰ or
- ▶ is for processing of personal data in service of scientific or statistical research according to Article 12 of the Draft PDP Decree.²¹¹

d. Scientific or statistical research

The Draft PDP Decree permits processing²¹² of de-identified personal data, and sharing of such data with a third party,²¹³ without the consent of data subjects for purposes of scientific or statistical research, subject to compliance with specific requirements.²¹⁴

Firstly, a personal data processor who wishes to rely on this legal basis to process personal data without consent must:

- ▶ give a commitment to protect personal data;²¹⁵
- ▶ take measures to secure personal data;²¹⁶
- ▶ have a physical device to protect personal data;²¹⁷
- ▶ have a specialized department assigned the task of protecting personal data;²¹⁸ and
- ▶ have registered to handle sensitive personal data with the Committee;²¹⁹

The personal data processor may only rely on the exception once it has received written confirmation from the Committee that it has complied with the above requirements.²²⁰

Secondly, before the data is used for these purposes, it must be de-identified by removing personally identifiable information, or pseudonymized by replacing personally identifiable information with a code to create new data that cannot identify a particular individual.²²¹

²⁰⁶ Draft PDP Decree, Article 6(1)(d).

²⁰⁷ Draft PDP Decree, Article 6(1)(d).

²⁰⁸ Draft PDP Decree, Article 10(2)(a).

²⁰⁹ Draft PDP Decree, Article 10(2)(b).

²¹⁰ Draft PDP Decree, Article 10(2)(c).

²¹¹ Draft PDP Decree, Article 10(2)(d).

²¹² Draft PDP Decree, Article 10(1)(e).

²¹³ Draft PDP Decree, Article 10(2)(d).

²¹⁴ Draft PDP Decree, Article 12.

²¹⁵ Draft PDP Decree, Article 12(4)(a).

²¹⁶ Draft PDP Decree, Article 12(4)(b).

²¹⁷ Draft PDP Decree, Article 12(4)(c).

²¹⁸ Draft PDP Decree, Article 12(4)(d).

²¹⁹ Draft PDP Decree, Article 12(4)(d).

²²⁰ Draft PDP Decree, Article 12(4)(e).

²²¹ Draft PDP Decree, Articles 12(2) and 2(13).

Thirdly, personal data to be used for scientific or statistical research purposes must be encrypted²²² and may be decoded exclusively for scientific or statistical research by specific persons designated in writing as having access to the information required for decryption.²²³

The Draft PDP Decree also prohibits aggregation of the results of processing personal data for scientific or statistical research into information that can identify a particular data subject.²²⁴

²²² Draft PDP Decree, Article 12(1).

²²³ Draft PDP Decree, Article 12(2).

²²⁴ Draft PDP Decree, Article 12(3).



ASIAN BUSINESS LAW INSTITUTE

The Asian Business Law Institute (ABLI) is a permanent think tank based in Singapore that initiates, conducts and facilitates research with a view to providing practical guidance in the field of Asian legal development and promoting the convergence of Asian business laws.

1 SUPREME COURT LANE | LEVEL 6 | SINGAPORE 178879

ABLI.ASIA | INFO@ABLI.ASIA



The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

1350 EYE STREET NW | SUITE 350 | WASHINGTON DC 20005

FPF.ORG | INFO@FPF.ORG