Privacy Compliance

VIETNAM DATA PROTECTION HANDBOOK

First Edition

March 2025

Table of Contents

Authors

Mr. Nguyen
Tech Lawyer | Arbitrator | CIPP/E

Mr. Pham
CIPM | CIPP/E | CISM | CRISC® | CISA | CC (ISC)2 | ISO 27001 LA | ISO31000

Ms. Giang Le
Ph.D in Law

Mr. Duc
Cybersecurity Expert

Ms. Hien Phan
Tech Lawyer | DPO

Mr. Anh Ngo
Associate | CIPP/E

Ms. An Pham
Privacy Associate

Disclaimer

This Handbook is drafted by the authors credited above for informational purposes only. The Handbook reflects the authors' personal opinions and does not represent the official view of **PrivacyCompliance**. It is not intended to act as and shall not be construed as an official legal opinion or consultation by **PrivacyCompliance**. The Handbook contains some contents that were collected, edited, compiled, and referenced from various sources by the authors. **PrivacyCompliance** and the authors do not claim ownership of the referenced materials and do not guarantee their validity, accuracy, or up-to-dateness.

"Personal data is the new oil of the internet and the new currency of the digital world."

Meglena Kuneva - European Consumer Commissioner

Introduction

The right to personal data stems from the right to privacy, which is considered a fundamental human right. Privacy is intricately woven into the fabric of modern societies, serving as a cornerstone for individual freedom, autonomy, and dignity. The Universal Declaration of Human Rights, adopted by the United Nations General Assembly in 1948, articulates the global commitment to safeguarding the inherent dignity and rights of every individual, in which the right to privacy is explicitly recognized in Article 12, where it is stated: *"No one shall be subjected to arbitrary interference with his privacy."* This international recognition sets the stage for our exploration of the personal data landscape of Vietnam.

In the Vietnamese context, privacy and by extension – personal data have undergone dynamic transformations, influenced by historical, cultural, and socio-political factors. With the advent of the digital age, the rapid proliferation of information and communication technologies has posed both opportunities and challenges to the protection of personal data. From the traditional norms of familial privacy to the contemporary implications of data protection and surveillance, Vietnam grapples with the delicate balance between technological advancements and individual rights.

To illustrate the relevance of personal data in Vietnam, it is essential to consider the impact of data-driven technologies on daily life. The collection and processing of personal information, while facilitating convenience and connectivity, also raise concerns about data security and the potential for misuse. Understanding these concerns is crucial for individuals, businesses, and policymakers alike.

Authorities play a pivotal role in shaping the personal data protection landscape. In this Handbook, we will explore the legal frameworks governing personal data protection in Vietnam, examining key legislation, regulations, and guidelines. By delving into these authoritative documents, readers will gain insights into the rights afforded to individuals and the obligations imposed on entities handling personal information.

In all, the goals of this Handbook are to empower individuals with knowledge, equip businesses with responsible practices, and to make recommendations to policymakers to shape a robust and adaptive legal framework. By understanding and examining Vietnam's unique situation and personal data protection legal landscape, we lay the foundation for a comprehensive exploration of personal data rights and responsibilities in the digital age.

Privacy Compliance

OVERVIEW OF

THE PERSONAL DATA LEGISLATION IN THE WORLD

Personal data protection around the world has had a long history. However, in recent years, with the advancement of technologies and the rise in people's awareness, there has been a significant increase in personal data protection regulations around the world.

Overview of the personal data legislation in the world

The EU

The European Union's General Data Protection Regulation (GDPR), which came into effect on May 25, 2018, is one of the most comprehensive and globally influential data protection laws to date. It replaced the EU's 1995 Data Protection Directive (Directive 95/46/EC), modernizing data protection laws to better address the realities of the digital age. The GDPR sets high standards for data privacy, creating a framework designed to protect individuals' personal data and privacy rights within the EU and beyond. By setting a global benchmark, the GDPR has inspired similar data protection laws around the world.

The GDPR applies broadly to the processing of personal data within the European Union. It also has an extraterritorial effect in certain cases. The GDPR grants extensive rights to data subjects (e.g. right to be informed, right to access, right to rectification, right to erasure, right to object, etc.), empowering individuals to control how their personal information is collected and used. These rights give data subjects more control and transparency regarding their personal information, establishing the GDPR as a robust data protection law. The GDPR sets requirements for ensuring the safeguard of personal data whether processed within the EU or transferred across borders.

The GDPR enforces compliance with significant penalties for non-compliance. Organizations that violate GDPR can be fined up to €20 million or 4% of their global annual turnover, whichever is higher, for the most serious infringements. Lesser infringements can result in fines of up to €10 million or 2% of annual turnover.[1] These high penalties underscore the EU's commitment to rigorous data protection standards, ensuring that data controllers and processors prioritize data security and privacy.

The GDPR has set a new global standard for data protection by establishing clear rules around data collection, processing, and transfer while giving individuals robust rights over their data. With comprehensive obligations for data controllers and processors, strict cross-border transfer rules, and substantial sanctions, the GDPR emphasizes transparency, accountability, and data security.

In addition to its immediate impact within the EU, the GDPR's influence has been felt worldwide, inspiring similar privacy laws in numerous countries and shaping international data protection practices. For organizations doing business in or with the EU, GDPR compliance is essential, as non-compliance carries significant legal and financial risks. As data continues to drive modern economies, the GDPR remains a landmark regulation, ensuring that privacy and data protection are fundamental rights in the digital era.

The US

In the United States, privacy and personal data regulations are largely governed at the state level, with the California Consumer Privacy Act (CCPA) serving as a leading example of comprehensive state privacy legislation. At the federal level, however, the U.S. currently lacks a unified privacy law comparable to the EU's GDPR. Instead, there is a patchwork of industry-specific and activity-specific federal laws, alongside ongoing discussions about draft federal privacy laws that could create a national framework.

The California Consumer Privacy Act (CCPA), is one of the most comprehensive state privacy laws in the U.S. and has become a model for other states considering similar legislation. The CCPA grants California residents a range of rights over their personal data, including: right to know; right to access; right to opt-out; and right against discrimination.

In 2023, the California Privacy Rights Act (CPRA) was enacted to expand on the CCPA, introducing additional requirements for data processing and creating the California Privacy Protection Agency (CPPA) to enforce and oversee privacy regulations. The CPRA adds rights like the right to correct personal data and imposes new obligations for businesses handling sensitive information, including restrictions on data sharing and enhanced disclosure requirements.

Other states, such as Virginia (Virginia Consumer Data Protection Act), Colorado (Colorado Privacy Act), and Connecticut (Connecticut Data Privacy Act), have since passed similar laws. These state-level regulations follow the example set by California but vary slightly in terms of rights granted, compliance obligations, and scope of applicability.

At the federal level, there is no single, comprehensive privacy law governing personal data protection across all sectors. Instead, there are several federal laws addressing specific types of data or sectors, such as (non-exhaustive list):

- Health Insurance Portability and Accountability Act (HIPAA): Governs the privacy and security of health information
- Children's Online Privacy Protection Act (COPPA): Protects the data privacy of children under 13 years of age
- Gramm-Leach-Bliley Act (GLBA): Requires financial institutions to protect customers' private data
- Fair Credit Reporting Act (FCRA): Regulates the use and accuracy of credit information

These sector-specific laws create baseline privacy protections within their domains but lack comprehensive reach, leaving many areas of data privacy unregulated.

In recent years, US Congress has seen growing momentum to enact a federal privacy law, which would address inconsistencies among state laws and create a standard across the country. While various bills have been proposed, two draft laws have gained significant attention such as:

The American Data Privacy Protection Act (ADPPA):

The American Data Privacy Protection Act (ADPPA): The ADPPA is a bipartisan bill that aims to establish a national privacy framework with provisions for data collection, transparency, consumer rights, and data security. The bill would preempt most state laws, creating a unified national standard. However, certain provisions are still under debate, such as enforcement mechanisms and whether the federal law should supersede state laws entirely.

The Consumer Online Privacy Rights Act (COPRA):

The Consumer Online Privacy Rights Act (COPRA): This proposed law, introduced by Democratic lawmakers, would provide similar protections to the ADPPA, focusing on consumer rights over personal data, transparency in data processing, and robust mechanisms for individuals to exercise their rights. COPRA includes provisions for both federal and state enforcement and would allow individuals to file lawsuits against companies for violations, making it one of the more stringent proposals.

While federal privacy legislation has yet to pass, the ongoing interest and bipartisan support for ADPPA indicate that a comprehensive privacy law may be on the horizon, reflecting a growing desire to create a consistent framework across states and industries.

China

China's Personal Information Protection Law (PIPL), which came into effect on November 1, 2021, represents the country's first comprehensive legislation dedicated to protecting personal information. The PIPL establishes a legal framework for data protection, sets guidelines for how organizations must handle personal data, and provides individuals with rights over their data. Inspired by international standards, such as the EU's GDPR, the PIPL aims to protect individuals' privacy and personal information in a rapidly digitizing environment.

The scope of the PIPL is broad, aside from applying to domestic entities, it also applies to those outside of China in some cases such as when the information is processed to provide products or services to individuals in China. There are some exceptions, however, particularly for personal information processed for personal/family affairs. This broad jurisdictional reach means that even foreign businesses dealing with Chinese residents' data are subject to PIPL requirements if they collect or process personal information within China's borders.

The PIPL grants data subjects a suite of rights similar to those seen in other global data privacy laws. Individuals, for example, have the right to access and correct their personal information, to request deletion under certain conditions, to withdraw consent, and to know how their data is being used. These rights aim to empower individuals and give them greater control over their personal information, helping them protect their privacy and monitor their digital footprint.

Data controllers and processors face several obligations under the PIPL, with specific requirements regarding the collection, use, storage, and protection of personal information. For instance, organizations must ensure they collect data lawfully, inform individuals about data collection and usage purposes, implement data security measures, and designate a data protection officer for oversight. Additional obligations apply to "important" data and sensitive personal information, such as data of children under 14 years old, which require stricter handling protocols and authorization processes.

To enforce compliance, the PIPL sets out a range of sanctions, including significant financial penalties for non-compliance, with fines reaching up to 5% of an organization's annual revenue or 50 million Yuan.[2] Severe breaches can lead to the revocation of business licenses, restrictions on management personnel, and even personal fines for responsible executives, highlighting the importance of adherence to the law.

In summary, China's PIPL is a landmark law that establishes a robust framework for data protection, aligning with global privacy standards while reflecting China's unique regulatory priorities. By defining clear rights for data subjects, outlining comprehensive obligations for data controllers and processors, and regulating data transfers and penalties, the PIPL aims to build a safer digital environment. For organizations operating within China or handling data of Chinese residents, compliance with the PIPL is essential, not only to avoid legal repercussions but also to build trust with customers and stakeholders in a rapidly evolving digital landscape.

Privacy Compliance

OVERVIEW OF

VIETNAM PERSONAL DATA REGULATIONS

Vietnam's privacy regulations are evolving, with the Personal Data Protection Decree currently serving as the main legal framework, emphasizing data subject consent and safeguarding personal data rights.

History of the Right to Privacy and Personal Data in Vietnam

1946 — Stated in the very first Constitution of Vietnam

1954-1980 — Declared in Law No. 103 - SL/L.005 (1957)

1980-1995 — Expanded the regulated scope in subsequent Constitutions

1995-2005 — Stated in the Civil Code (1995 and 2005)

2013~ — Comprehensively regulated in 2013 Constitutions và the 2015 Civil Code

The right to privacy in Vietnam could be traced back to the right to private life, personal secrets, and correspondence. In the very first Constitution of Vietnam written in 1946, it is stated that the homes and correspondence of Vietnamese citizens shall not be illegally violated.[3]

During the period from 1954 to 1980, when northern Vietnam was fully liberated and focused on socialist-oriented economic development, the State enacted Law No. 103 - SL/L.005 in 1957. This law guaranteed the physical liberty of citizens and their inalienable rights regarding housing, property, and correspondence. The 1985 Criminal Code also addressed the privacy of correspondence and residence-related personal information, but other aspects of personal information remained unaddressed. In all, before 1986, the protection of personal information in Vietnam was acknowledged in principle. However, specific regulations regarding its definition, the rights and obligations of individuals, the scope of protection, and related procedures were lacking. Criminal penalties for violations of personal information were limited to issues concerning residence and correspondence. [4]

The right to privacy has been maintained and improved through the subsequent 04 versions of the Vietnamese constitution. Article 11 of the 1946 Constitution only mentioned the inviolability of correspondence, however, the 1959 Constitution (Article 28), the 1980 Constitution (Article 71), and the 1992 Constitution (Article 73) expanded the scope of this right. The extent of this expansion reached its most comprehensive form in the 2013 Constitution in which it is stated that:

- *Everyone has the right to inviolability of private life, personal secrets and family secrets; and has the right to protect his or her honor and reputation. The security of information about private life, personal secrets or family secrets shall be guaranteed by law.*
- *Everyone has the right to privacy of correspondence, telephone conversations, telegrams and other forms of private communication.*
- *No one may illegally break into, control or seize another's correspondence, telephone conversations, telegrams or other forms of private communication." [5]*

The right to privacy is also stipulated in other legal documents, with the most prominent being the Civil Code. The Civil Code is one of the foundational legal documents that govern the personal and property relations of the subjects participating in civil legal relations. The Code is the basis for many other legal documents. The first Civil Code of Vietnam was issued in 1995 and included a provision protecting the right to privacy of the individual.[6] This right is further reinforced in the Civil Code 2005 and in the latest iteration - the Civil Code 2015, in which it is stated that:

- *The private life, personal secrets and family secrets of a person are inviolable and protected by law.*
- *The collection, preservation, use and publication of information about the private life of an individual must have the consent of that person; the collection, preservation, use and publication of information about the secrets of the family must have the consent of all family's members, unless otherwise prescribed by law.*
- *The safety of mails, telephones, telegrams, other forms of electronic information of an individual shall be ensured and kept confidential.*
- *The opening, control and keeping of mails, telephones, telegrams, other forms of electronic information of an individual may only be conducted in cases provided by law.*
- *Contracting parties of a contract may not disclose information about each other's private life, personal secrets or family secrets that they know during the establishment and performance of the contract, unless otherwise agreed."*

The right to privacy could also be found in other sector-specific regulations throughout the years such as the Law on People's Health Protection 1989, Law on E-transaction 2005 (replaced by the 2023 version), Law on Information Technology 2006, Telecommunications Law 2009 (replaced by the 2023 version), HIV/AIDS Prevention and Control Law 2006, Law on Protection of Consumers' Rights 2010 (replaced by the 2023 version), etc.

The inclusion of the right to privacy in every version of the constitution as well as core legal documents such as the civil code and other sector-specific laws shows that privacy has always been a concern of lawmakers for nearly 70 years.

Current Legal Documents Governing Privacy and Personal Data in Vietnam

According to the Ministry of Public Security ("**MPS**")[7], as of 2023, there are a total of 69 legal documents directly related to personal data protection in Vietnam, including the Constitution; 04 Codes; 39 Laws, 01 Ordinance; 19 Decrees; 04 Circulars/Joint Circulars; and 01 Decision of the Minister. However, although there are up to 69 documents, all of them do not agree on the concept and content of personal data and personal data protection. The term "personal data/information" appears in more than 300 legal documents but with only 07 definitions.[8] Prominent documents with the widest scope and effect among these include:

- Civil Code No. 91/2015/QH13;
- Criminal Code No. 100/2015/QH13, as amended from time to time;
- Law No. 32/2024/QH15 on Credit Institutions;
- Law No. 24/2018/QH14 on Cybersecurity;
- Law No. 86/2015/QH13 on Cyber-Information Security;
- Law No. 19/2023/QH15 on Protection of Consumers' Rights;
- Law No. 67/2006/QH11 on Information Technology;
- Law No. 20/2023/QH15 on E-transactions;
- Law No. 102/2016/QH13 on Children;
- Decree No. 53/2022/ND-CP of the Government elaborates a number of articles of the Law on Cybersecurity of Vietnam;
- Decree No. 91/2020/ND-CP of the Government on anti-spam messages, emails and calls;
- Decree No. 15/2020/ND-CP of the Government on penalties for administrative violations against regulations on postal services, telecommunications, radio frequencies, information technology and electronic transactions;
- Decree No. 98/2020/ND-CP of the Government on penalties for administrative violations against regulations on commerce, production and trade in counterfeit and prohibited goods, and protection of consumer rights; as amended by Decree No. 17/2022/ND-CP and Decree No.24/2025/ND-CP; etc.

All of this shows that Vietnam's legislation on personal data protection is currently very fragmented with no clear, universal direction. This is in contrast to other more developed countries where personal data legislation has been around for a long time, such as the GDPR of the EU. That is until recently when the Vietnamese government issued Decree 13/2023/ND-CP on the protection of personal data ("**PDPD**"). This is currently the most comprehensive legal document in Vietnam governing personal data processing. The PDPD was issued on 17 April 2023 and went into effect on 01 July 2023 without any grace period. For the first time, a legal document in Vietnam sets out general definitions regarding personal data, the principles of personal data processing, and the rights and obligations of the data subjects, data controllers, and processors. The PDPD is the first legal document to apply to all personal data across different sectors. Its issuance has caused quite a stir among enterprises in the country, especially the banking and insurance industries, considering the nature of their sectors and the burden of compliance the PDPD brings. The issuance of the PDPD somewhat mitigated the situation by setting up the general concepts and principles of personal data protection, however, it was not enough considering its effect is still below that of other laws. In addition, PDPD does not supersede the regulations on personal data protection set out in other legislations, therefore, it also raises concerns about potential conflicts and the priority of the PDPD over other sub-law documents.

Aside from the PDPD, there is also a draft decree on sanctions regarding cybersecurity and personal data violations that is currently in the work and is expected to be issued in the future. Furthermore, in September 2024, the MPS publicized the first draft of the Personal Data Protection Law in order to further reinforce the current regulations and give them more power, the latest version was released on 10 March 2025. It is expected that the Personal Data Protection Law will be officially adopted in May 2025 and take effect from 2026, however, such a date could be subject to change. Vietnam also recently issued the Data Law 2024 on November 30, 2024, however, this law focuses primarily on developing and managing digital data, databases, providing data to the government, and data products and services with little to no mention of personal data or privacy rights. According to the Draft Decree Detailing the Data Law (publicized on 16 January 2025) and the Draft Decision on the Classification of Crucial and Core Data (publicized on 23 January 2025), personal data when reaching a certain threshold (e.g. data on 50,000 or more cross-border banking transactions, basic personal data of 1 million or more people, sensitive personal data of 10,000 or more people, etc.) will be considered "crucial" or "core data" and will be subject to certain procedures under the Data Law such as risk assessments, impact assessments when being transferred, processed outside of Vietnam.

In all, the right to privacy and personal data in Vietnam is at a turning point in which the government is ramping up its efforts to effectively regulate this new resource

Privacy Compliance

VIETNAM

PERSONAL DATA REGULATIONS

The most comprehensive personal data protection legislation in effect in Vietnam at the moment is the PDPD. This section will go over the provisions of the PDPD and their applications. The Handbook will also present relevant revisions or new provisions of the Draft Personal Data Protection Law.

Scope

The PDPD boasts an incredibly wide scope. The PDPD covers all matters relating to personal data protection and the responsibilities of relevant agencies, organizations and individuals for personal data protection.[9]

The PDPD also applies to a wide range of subjects which include:[10]

- Vietnamese agencies, organizations and individuals;
- Foreign agencies, organizations and individuals being based in Vietnam;
- Vietnamese agencies, organizations and individuals operating overseas;
- Foreign agencies, organizations and individuals directly participating in or involved in the personal data processing in Vietnam.

This means that the PDPD has extra-territorial effect and can affect even foreign entities as long as they are involved in personal data processing in Vietnam. Furthermore, different from the EU's GDPR, the PDPD has no exemption for any entity or purpose, meaning that personal data processing on a personal or household level of individuals would, technically, have to comply with the PDPD which is, admittedly, hard to imagine.

Definitions

Personal data, processing personal data

Personal data

"Personal data means any information that is expressed in the form of symbol, text, digit, image, sound or in similar forms in electronic environment that is associated with a particular natural person or helps identify a particular natural person. Personal data includes basic personal data and sensitive personal data."[11]

This is a fairly straightforward definition of personal data. Also from the definition, we can conclude that personal data can only be data of a natural person, and data on organizations and businesses would not be considered personal data (e.g. the name of a corporation is not personal data unless it contains elements relating to a natural person).
It is also stated that there are two categories of personal data: basic and sensitive. Sensitive personal data is defined as personal data associated with an individual's privacy that, when being infringed upon, shall cause a direct effect on the legitimate rights and interests of such individual which include data on political and religious views, health information, racial and ethnic origins, customer information held by credit institutions, etc.[12] On the other hand, basic personal data is defined simply as personal data that is not sensitive, such as name, date of birth, gender, photos, etc.[13]

Personal Data Processing

As for data-related activities, *"personal data processing means one or more operations that affect personal data, such as: obtaining, recording, analysis, confirmation, storage, alteration, publication, combination, access, retrieval, recovery, encryption, decryption, duplication, sharing, transmission, provision, transfer, deletion, destruction of personal data or other relevant operations."*[14]

This means that any operations that affect personal data shall be construed as personal data processing. Thus, in reality, as long as an entity interacts with personal data, it is extremely likely that such an entity will be considered as engaging in personal data processing.

Entities Involved in Personal Data Processing

Data Subject

"Data subject means an individual identified by personal data"[15]

This further solidifies the fact that personal data only includes data of natural people and not of businesses and corporations. Furthermore, the processing of the personal data of deceased individuals is also subject to this regulation as detailed later below.

Entities Involved in Personal Data Processing

Data controller	"*Data controller means an organization or individual that decides on the purpose and means of personal data processing.*"[16] The "*purpose*" here could be understood as the reason for which the personal data is being processed (e.g. for marketing, research, employee management, etc.). The "means" could be understood as the specifics of the processing itself (e.g. what data is collected, how long the data will be kept, when it will be erased, etc.).
Data processor	"*Data processor means an organization or individual that performs the processing of the data on behalf of a data controller under a contract or agreement with such data controller.*"[17] This means that the data processor is merely carrying out the processing activities on behalf of the data controller via an agreement. Therefore, the data processor cannot process personal data for its own purposes, if it does, it would be considered a data controller in the scope of such processing activities.
Data controller-cum-processor	"*Data controller-cum-processor means an organization or individual that decides on the purpose and means of processing and simultaneously and directly performs the personal data processing.*"[18] This entity would act as both the data controller and the data processor and shall have the rights and obligations of both entities. This type of entity is unique to the PDPD. In other personal data regulations around the world such as the GDPR, it is implied that the data controller also processes personal data to a certain degree. The main difference between data controllers and data processors is that data processors process personal data on behalf of others and not for their own purposes. In reality, the cases where a party only decides the purposes and means of processing without actually processing the data itself are quite few in number since the collection of data is already a processing activity.
Third party	"*Third-party means an organization or individual other than the data subject, data controller, data processor, and controller-cum-processor that is authorized to process personal data.*"[19] This is an especially peculiar entity. From the definition above, it would be reasonable to assume that this entity has the ability/the right to process personal data but does not decide the purposes and means of processing nor does it process personal data on behalf of another party. An example of a "third party" could, therefore, be state authorities since they may have the power to process personal data given to them by the laws but are not currently processing the data. There has not been a unified definition or clear examples of third party given by the authorities, as such, identifying this entity in the course of everyday business remains a challenge.

Cross-border transfer of personal data

"Cross-border transfer of personal data means any activity involving the use of cyberspace, electronic equipment, electronic means or other forms to transfer personal data of Vietnamese citizens to a location outside the territory of the Socialist Republic of Vietnam or use of a location outside the territory of the Socialist Republic of Vietnam to process a Vietnamese citizen's personal data, including:

- *Organizations, enterprises or individuals transferring personal data of Vietnamese citizens to organizations, enterprises or management bodies located overseas for processing in accordance with the purposes consented by the data subjects;*
- *Processing of personal data of Vietnamese citizens by use of automated systems located outside the territory of the Socialist Republic of Vietnam by the data controller, data controller-cum-processor or data processor in accordance with the purposes consented by the data subjects."*[20]

In short, cross-border transfer of personal data means either the transfer of personal data outside the territory of Vietnam (e.g. a company transferring the personal data of its employees to its mother company outside of Vietnam) or the usage of automated systems outside of Vietnam to process personal data (e.g. a company using a cloud storage system to store its employees' information in an oversea server). This provision only applies to the transfer of personal data of Vietnamese citizens.

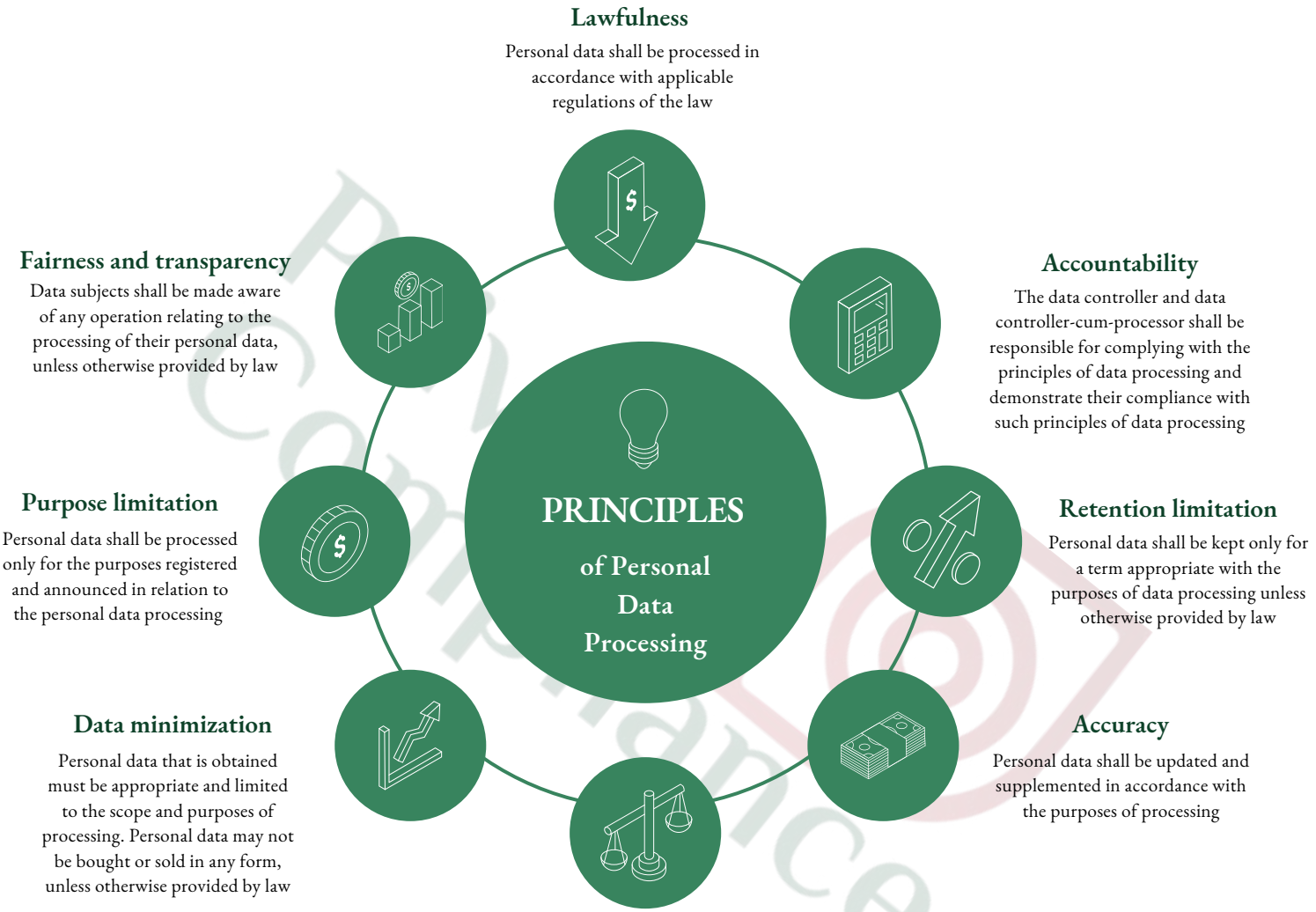
Consent

"Consent of the data subject means an explicit, voluntary and affirmative expression of the permission of a data subject for the processing of their personal data."[21]

This is one of the bases and the most common one allowing personal data processing in which the data subject clearly and voluntarily allows for their personal data to be processed.

Principles of Personal Data Processing

The principles for personal data protection in Vietnam are prescribed in Article 3 of the PDPD which includes eight (08) principles as follows:



Lawfulness

Personal data shall be processed in accordance with applicable regulations of the law

Accountability

The data controller and data controller-cum-processor shall be responsible for complying with the principles of data processing and demonstrate their compliance with such principles of data processing

Retention limitation

Personal data shall be kept only for a term appropriate with the purposes of data processing unless otherwise provided by law

Accuracy

Personal data shall be updated and supplemented in accordance with the purposes of processing

Integrity and confidentiality

Personal data shall be subject to protection and security measures during the processing, including protection against violations of the regulations on personal data protection and prevention and control of loss, destruction or damage caused by incidents, using technical measures

Data minimization

Personal data that is obtained must be appropriate and limited to the scope and purposes of processing. Personal data may not be bought or sold in any form, unless otherwise provided by law

Purpose limitation

Personal data shall be processed only for the purposes registered and announced in relation to the personal data processing

Fairness and transparency

Data subjects shall be made aware of any operation relating to the processing of their personal data, unless otherwise provided by law

Rights and Obligations of Data Subjects

Rights [22]	• Right to be informed: Data subjects shall be made aware of any operation of processing of their personal data; • Right to consent: Data subjects may or may not consent to the processing of their personal data; • Right to access [to information]: Data subjects may access to view, edit or request to edit their personal data; • Right to withdraw consent: Data subjects may withdraw their consents; • Right to delete data: Data subjects may delete or request for deletion of their personal data; • Right to restrict data processing: Data subjects may request to limit the processing of their personal data; • Right to provision of data: Data subjects may request the data controller or the data controller-cum-processor to provide them with their own personal data; • Right to object to data processing: Data subjects may object to the processing of their personal data by the data controller or data controller-cum-processor to prevent or limit the disclosure of their personal data or the use of their personal data for advertising or marketing purposes; • Right to complain, denounce and/or initiate lawsuits: Data subjects may complain, denounce or initiate lawsuits in accordance with the law; • Right to claim damages: Data subjects are entitled to claim damages in accordance with the law upon violation of the regulations on personal data protection unless otherwise agreed by the parties or prescribed by law; • Right to self-defense: Data subjects are entitled to self-defense in accordance with the Civil Code, other relevant laws, and the PDPD, or may request competent agencies or organizations to implement the measures for the protection of civil rights as prescribed in Article 11 of the Civil Code. The particulars of the performance of these rights shall be detailed below regarding the obligations of the data controllers and data processors.
Obligations [23]	• To self-protect their own personal data; to request other relevant organizations and individuals to protect their personal data; • To respect and protect others' personal data; • To fully and accurately provide personal data upon giving consent to the personal data processing; • To participate in the propaganda and dissemination of skills for personal data protection; • To comply with the law on personal data protection and participate in the prevention of and fight against violations of the regulations on personal data protection.

Administrative Procedures

Conducting Privacy Impact Assessments

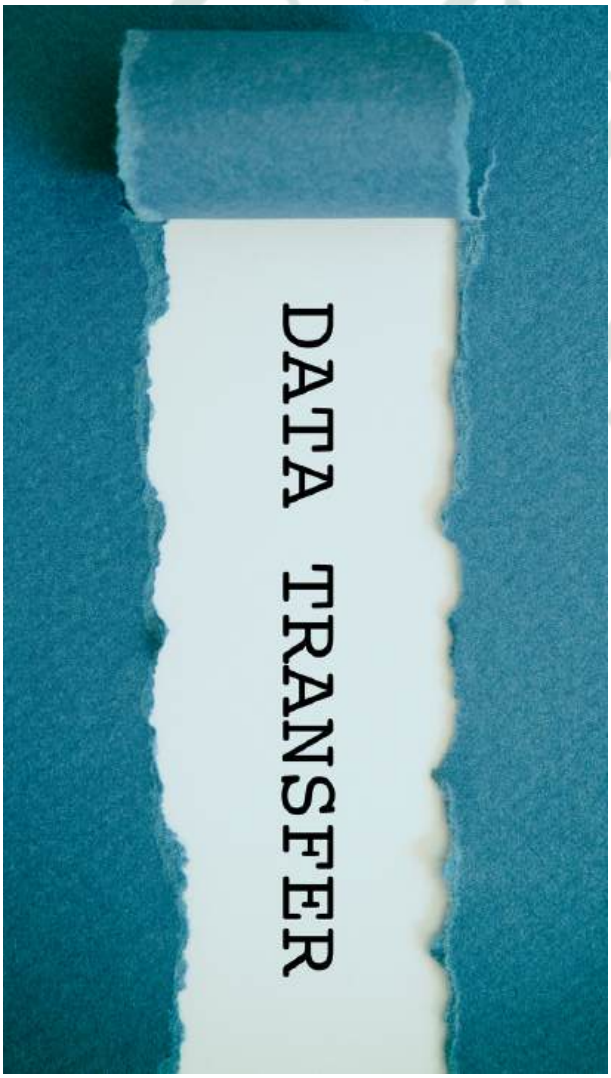
The data controller and the data processor are required to conduct a personal data processing impact assessment ("**DPIA**") and a cross-border transfer impact assessment ("**DTIA**") (if the data controller/processor transfers the personal data of Vietnamese citizens abroad). Also in cases where there are changes made to the dossiers, such changes must also be notified to the competent authorities. Please refer to the table below for details regarding the procedures.

	DPIA	DTIA	Amending the Dossiers
Applicable Subjects	Data controllers/data controller-cum-processors and data processors.	The party transferring the personal data of Vietnamese citizens abroad, regardless if that party is the data controller, data controller-cum-processor, data processor, or third party.	The party which drafted the dossiers.
Form	Both data controllers and data processors use Form No. 4 attached to the PDPD to notify the submission of the DPIA. The forms used for the DPIA shall be the form D24-DLCN-01 (for data controllers/data controller-cum-processors) and form D24-DLCN-02 (for data processors). Both of which are attached to the Decision No. 4660/QĐ-BCA-A05. There is also form D24-DLCN-03 for third parties, however, PDPD does not stipulate that third parties must carry out DPIA. This matter is currently unclear.	The data transferring party shall use Form No. 6 attached to the PDPD to notify the submission of the DTIA. The form used for the DTIA shall be D25-DLCN-04 attached to Decision No. 4660/QĐ-BCA-A05.	Form No.6 attached to the PDPD.

	DPIA	DTIA	Amending the Dossiers
Validity	The dossier shall be prepared in a legally valid document of the data controller, data controller-cum-processor, or data processor.[24]		
Procedures	The dossier shall be kept and made available at all times for inspection and evaluation by the MPS and one (01) original copy shall be sent to the Ministry of Public Security (Department of Cybersecurity and Hi-tech Crime Prevention) ("**A05**").[25] [26]		The notification of changes made to the dossiers along with accompanying documents shall be sent to A05.[27]
Methods of Submission	• Online: at the National Personal Data Protection Portal. However, as of now, this method is not available since the portal does not support online submission; [28] • In person: submit the dossier in person at A05; • Via post.		
Time of Processing	10 working days (**Note**: In reality, the actual time for the authorities to process the dossier or the notification would be much longer)		
Time Limit for Compliance	60 days from the date of processing personal data.[29] [30] If the processing is conducted before the PDPD takes effect, the deadline will be 60 days from the date of the PDPD goes into effect (1 July 2023) – which has long passed.		10 days from the date the change is made.[31]

Notifying Cross-border Data Transfers

The party transferring the data abroad shall notify A05 in writing regarding the data transfer and contact information of organizations, and individuals in charge after the transfer has been completed.[32] However, in reality, data transfer happens daily and can be as simple as sending an email to a recipient abroad. As such, it is currently unclear when this notification is supposed to be made or how it is supposed to be made since there is no notification form or time limit for this procedure.



Data Protection Officer (DPO) Information Provision

As one of the protection measures for processing sensitive personal data, entities shall appoint a department responsible for the protection of personal data, designate personnel in charge of personal data protection, and communicate information about the department and individual responsible for personal data protection to the competent personal data protection authority – A05. In cases where the personal data controller, the personal data controller-cum-processor, the data processor, or a third party is an individual, the information of the individual performing the task shall be provided.[33] In practice, the provision of information about the DPO is included by businesses in the DPIA and DTIA dossiers rather than as a separate administrative procedure.

Reporting Violations of Personal Data Protection Regulations

Obligation

Upon detection of a violation of the regulations on personal data protection, the data controller or the data controller-cum-processor shall notify the A05 within 72 hours of the occurrence of the violation by filling out Form No. 03 set out in the Appendix of the PDPD.[34]

In case of notifying after 72 hours, the reason for delay or late notification must be included. The data processor shall be obligated to notify the data controller as soon as possible[35] upon becoming aware of a violation of the regulations on personal data protection, as such, it would be prudent for the controller to include a provision on the time limit for breach notification for the data processor. In practice, the data controllers usually set the reporting period within 24 hours or 48 hours from the violation detection to ensure their own ability to comply with the statutory notification timeframe.

Notification content

The notification shall include the following:[36]

- Descriptions of the nature of the violation of the regulations on personal data protection, including: time, location, acts, organizations, individuals, types of personal data and the amount of related data involved;
- Contact details of the staff assigned to data protection or organizations or individuals responsible for personal data protection;
- Descriptions of the possible consequences and damage caused by the violation of the regulations on personal data protection;
- Descriptions of the measures put in place to handle and minimize the harm of the violation of the regulations on personal data protection.

The information regarding the breach above could be split into multiple installments or stages in case they cannot be fully notified at once.[37]

Occurrence minutes

The data controller and/or data controller-cum-processor shall prepare written minutes confirming the occurrence of the violation of the regulations on personal data protection, and coordinate with the A05 to handle the violation.[38]

Others' obligation

Organizations and/or individuals shall notify the A05 upon detection of the following cases, regardless of their role in data processing:[39]

- There are violations of the law with respect to personal data;
- The personal data is processed for improper purposes or not in accordance with the original agreement between the data subject and the data controller and/or the data controller-cum-processor or in violation of the law;
- The rights of the data subject are not guaranteed or are not properly implemented;
- Other cases as prescribed by law.

PDPD requires that all violations, whether serious or minor, must be reported without exception, along with a 72-hour limit for reporting. This has made compliance with this regulation extremely challenging in practice.

Consent for Personal Data Processing

The PDPD stipulates that data subjects may or may not consent to the processing of personal data, except for the cases specified in Article 17 of the PDPD.[40] In addition, the PDPD also stipulates that the consent of the data subject applies to all activities in the personal data processing process unless otherwise provided by law.[41] The controller/controller-cum-processor is responsible for obtaining the consent of the data subject for all personal data processing activities before performing the processing. Note that the data subject's consent does not allow the data controller to process personal data contrary to the principles of personal data protection specified in Article 3 of the PDPD.

Information to Provide When Obtaining Consent

The consent of the data subject is only valid if it is voluntary and the data subject is aware of the following information:[42]

- Type of personal data to be processed (basic or sensitive personal data);
- Purpose of processing personal data;
- Organizations and individuals allowed to process personal data;
- Rights and obligations of data subjects.

Thus, when these contents change, the data controller must seek the consent of the data subject before processing personal data according to the changed contents.

Methods of Obtaining Consent

The consent of the data subject must be expressed clearly and specifically in writing, voice, by checking the consent box, via text message, selecting consent technical settings, or via other actions that demonstrate this.[43] Data subject's consent must be expressed in a format that can be printed, reproduced in writing, including in electronic or verifiable format.[44] The most important element in the form of consent is the ability to demonstrate consent later on. Thus, the form of consent collection needs to be designed to store relevant information and be able to demonstrate that the data subject has been provided with the legally required information and that the data subject has agreed to allow the processing of personal data.

Requirements for Valid Consent

The consent of the data subject must be clear, voluntary, and affirm the data subject's permission to process data

- Clear

The consent of the data subject must clearly demonstrate the data subject's will to allow the data processing. This condition can be met by designing the consent content separately from other contents, presenting it clearly and coherently, and using simple, easy-to-understand language.

- Voluntary (given freely)

Voluntary can be understood as the data subject making his/her own decision to agree to data processing after being provided with accurate information and without being threatened. However, voluntary can also be understood that the data subject will not suffer any consequences arising from not agreeing to the processing of personal data. For example, a data controller requires customers to provide personal data to sign a service contract. In it, the data controller requires the customer to provide information about the customer's online activities even though this data is not necessary for the conclusion of the contract and states that if the customer does not provide this information, the data controller will not sign the contract with the customer. In this case, even if the customer has consented to the processing of such data, the consent may be considered involuntary since the customer has been forced to provide the information, otherwise the contract would not be signed.

- Affirmative

The consent of the data subject must be an intentional, proactive action affirming the will of the data subject. The means of obtaining consent must be able to clearly demonstrate that the data subject has consented to the processing of personal data. Thus, the data controller should not employ methods of asking for consent that lack proactiveness from the data subject such as applying pre-checked consent boxes or declaring that the data subject’s continued use of the service constitutes consent to data processing. Especially, the data subjects’ silence or non-response shall not constitute consent.[45]

The consent must be given for the same purpose. When there are multiple purposes, the data controller, data controller-cum-processor must list out the purposes so that the data subject can agree to one or more of the stated purposes.[46]

This is part of the voluntary element of consent. In which, data subjects must have the right to consent to one or more purposes of processing personal data. The data controller must not force the data subject to agree to all processing purposes otherwise it will not process the data subject's personal data in a "*take-it-or-leave-it*" manner because this can be considered a form of forcing the data subject to agree to the conditions set by the data controller.

The data subject may give partial consent or with accompanying conditions [47]

Currently, the law does not clearly regulate this issue, so it is difficult to analyze the regulations or speculate on how they will apply in practice. However, through the language of the provision, it can be understood that data subjects will have the ability to consent to certain personal data processing activities and can set requirements that the data controller must meet in order to process the personal data. However, the practical implications of such interpretations are unclear.

Exemptions from Obtaining Consent

The PDPD also stipulates cases where the handling of personal data does not require the consent of the data subject, including:[48]

- in an emergency, it is necessary to immediately process relevant personal data to protect the life and health of the data subject or other people. It is the responsibility of the data controller, data processor, data controller-cum-processor, and third party to prove this case;
- disclosure of personal data in accordance with the law;
- data processing by competent state agencies in the event of an emergency regarding national defense, national security, social order and safety, major disasters, and dangerous epidemics; when there is a threat to security and national defense but not to the extent of declaring a state of emergency; to prevent and combat riots, terrorism, prevent and combat crimes and violations of the law according to the provisions of law;
- to perform the data subject's contractual obligations with relevant agencies, organizations and individuals according to the provisions of law;
- serving the activities of state agencies regulated by specialized laws.

In addition, competent agencies and organizations are allowed to record audio, video and process personal data obtained from audio and video recording activities in public places for the purpose of protecting national security, social security and order, legitimate rights and interests of organizations and individuals according to the provisions of law without the consent of the subject.

When making audio or video recordings, competent agencies and organizations are responsible for notifying the subject so that they understand that they are being audio or video recorded, unless otherwise prescribed by law.[49] However, currently, there is no clear definition of public places.

The scope of the exceptions mentioned above is quite narrow and as such, cannot cover all of the real-life cases where consent should be waived such as processing data for pre-contractual purposes, for carrying out contractual obligations of both sides, for legitimate interests, etc. like with the GDPR. This has led to an over-saturation of consent even when it is unnecessary.

Some specialized laws also stipulate cases where consent is not required when processing personal data such as IT, consumer rights protection, e-commerce, etc. These exceptions differ from the PDPD, raising the question of whether these sector-specific regulations can be applied alongside the PDPD's exceptions or whether the PDPD should take precedence as the most comprehensive legal instrument on personal data protection.

Informing the Data Subjects of the Processing

Notification is carried out once before proceeding with the processing of personal data.[50] This notification procedure is a separate activity from obtaining data subjects' consent and is for the purpose of providing information about the processing of personal data and does not have the purpose of obtaining consent. However, the notification shall not be required if the data subject has acknowledged and given consent to all of the contents of the notification before authorizing the data controller and data controller-cum-processor to collect his/her personal data.[51] As such, it is often recommended to include the notification information in the consent form to avoid having to perform a separate notification.

Contents of Notification

Contents of the notification to data subjects about personal data processing include:[52]

- Purpose of processing;
- The type of personal data processed relevant to the purpose of processing (basic or sensitive data protection);
- Processing method (automatic or manual processing, etc.);
- Information about other organizations and individuals related to the processing purpose (may include organizations to which data is transferred to carry out the processing purpose such as data processors, data recipients, etc.);
- Unwanted outcomes, damage that is likely to occur (data lost, stolen, counterfeited, etc.);
- Start time and end time of data processing.

In addition, according to Article 21(2)(a) of the Information Technology Law 2006, the data subject must also be informed about the form and location of collecting, processing, and using personal information.

While there are exceptions to the obligation to obtain consent as stated above, there are currently no such equivalents for the notification duty. This presents a number of issues such as in cases of emergency where the data subject cannot be notified of the information.

Format of Notification

Similar to consent, notification to the data subject must be in a format that can be printed, reproduced in writing, including in electronic or verifiable format.[53]

Processing Data in Special Cases

Processing Data of Individuals Declared Missing or Dead

In this case, because the data subject is not present, if the data controller wants to process the personal data of the data subject, it will have to get the consent of that person's spouse or adult children, in case such people are not present, it must get the consent of the father or mother of the person declared missing or deceased, except in cases where consent is not required according to Articles 17 and 18 of the PDPD.[54] Where all aforementioned individuals are absent, there could be no consent.

Processing Data for Marketing Purposes

Organizations and individuals engaged in marketing and product promotion services may only use customers' personal data collected through their business activities for marketing and product promotion services with the consent of the data subject.[55] Furthermore, the consent of the data subject must be based on the basis that the data subject clearly knows the content, method, form, and frequency of the advertisement. [56]

Processing Personal Data of Children

Children, defined as individuals under the age of 16, are explicitly recognized as data subjects under data protection law. Their personal data is processed frequently, necessitating robust privacy safeguards. While the PDPD defines the personal data of all subjects as information associated with an individual or used to identify an individual, Decree No. 56/2017/ND-CP ("Decree 56") adds more information of children to the scope of being protected, such as, personal property, address of and information on school, class, learning result and friends of the child; and information on services provided for the child. Such information, together with personal data, is referred to as "*private information of children*". To be permitted to use such information (especially on the online environment), organizations and service providers need to meet the special demands of the Decree 56.

Inheriting such spirit, the PDPD requires the personal data of such data subjects to be processed in a way that ensures their rights and best interest.[57] This principal regulation has been detailed by requirements on consent and age verification, as well as the deletion obligation in some special cases.

Consent for Processing Children's Personal Data

Obtaining valid consent is a pivotal step in processing children's personal data. Previously, Decree 56 required the consent of both parents/guardians and children aged 07 and older. The PDPD further underscores the importance of valid consent, particularly when it serves as the legal basis for processing. This process empowers both children and their parents/guardians to participate in decision-making and exercise control over their personal data.

To ensure the validity of consent obtained from children, the PDPD imposes additional requirements beyond those applicable to adult data subjects. Specifically, it may necessitate dual consent from both parents/guardians and children aged seven or older. This dual consent mechanism is designed to safeguard the interests of the child by preventing the overruling of any party's opinion during data processing, thus balancing the child's rights, safety and aspirations. The PDPD sets 07 years old as the age at which consent from children can be obtained, which is the same age as that outlined in Decree 56 and the Law on Marriage and Family.[58] Regarding children below such age, the sole consent from parents/guardians is considered valid for the data processing.

In addition, the PDPD requires age verification prior to the processing of a child's personal data. This responsibility is applied to not only the data controller (and processor) but also the processor and the third party.

The PDPD does not dictate specific verification techniques, but allows these parties to select suitable verification methods to implement, subject to the accountability obligations in Article 3(8). Proposed measures for verifying a child's age (based on guidance from the European Commission), include asking questions that children under seven are not able to answer or requiring written confirmation from the guardian.[59]

Deleting Children Personal Data

In the realm of data processing, apart from fulfilling conditions for obtaining consent, to optimally safeguard the rights and interests of children, the data controllers (and processors) are mandated to carry out the data erasure or data deletion in certain cases.

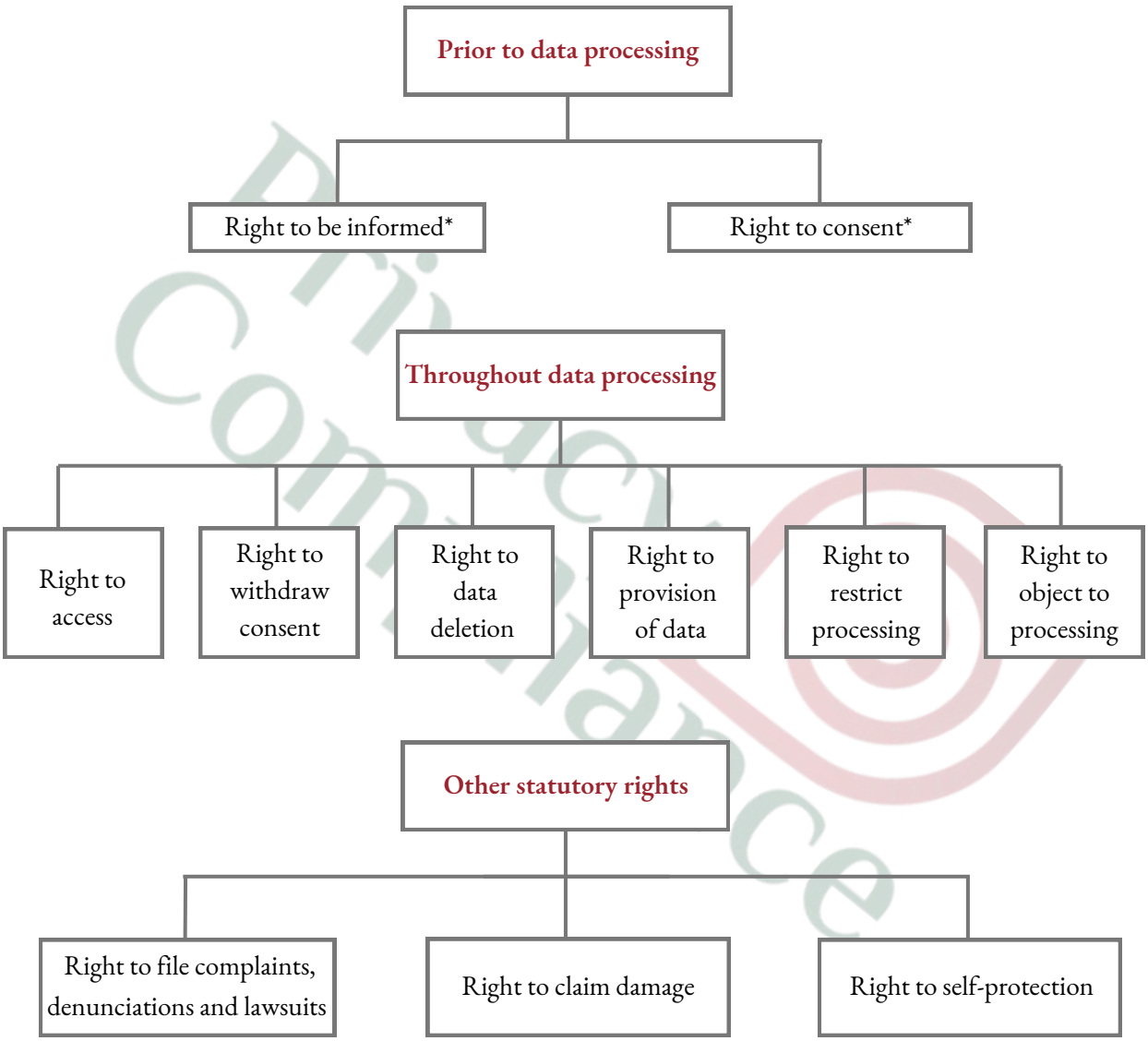
Specifically, participants must stop processing, irrevocably delete, or destroy a child's personal data in the following situations, unless otherwise provided by laws:

- When the personal data of the child is processed for purposes other than those notified, or when the purposes have been fulfilled.
- When a parent or guardian of the child withdraws consent.
- When requested by a competent authority, provided there is sufficient evidence that the processing has been detrimental to the legitimate rights and interests of the child, meaning a violation of the principle of protecting the best interests of the child.

However, regarding a child's right to withdraw consent. There is a gap in the current legal framework due to the lack of direct regulation on consequences when the child reaches the age of consent. While the law requires consent from both the guardian and the child aged 07 and older, the process of withdrawing consent, as stipulated in Article 20(3) of the PDPD, only applies to the child's parents or guardian. This provision contradicts the principle of children's best interests by disregarding the child's opinion on withdrawing consent. This limitation raises the question about whether children, once they have the full status of a data subject, have the right to modify or withdraw consent that was initially given by their guardian. In essence, when a child reaches the specified age, they should possess all the rights of a data subject, including the right to withdraw consent. However, the fact that this consent was not given by the children themselves, but by another party, raises the possibility of whether only the person who gave the consent can withdraw it. The lack of specific regulations on this matter hinders practical implementation and may lead to disputes between data subjects and controllers due to differing interpretations of the law.

Handling Data Subjects' Right Requests

(*): aforementioned



Right to Access [60]

Data subjects shall be entitled to:

- Have access to view and correct their personal data collected by the data controller or the data controller-cum-processor under their consent, unless otherwise provided by law;
- Request the data controller or the data controller-cum-processor to correct their personal data where the personal data cannot be corrected directly [by the data subjects] due to technical or other reasons.

The data controller or the data controller-cum-processor shall correct the data subjects' personal data as soon as possible after the data subjects have given consent thereto or in accordance with specialized laws.

The data processor and the third party may correct the data subjects' personal data after obtaining the written consent of the data controller or data controller-cum-processor with the awareness that the data subjects have given the same.

Right to Withdraw Consent [61]

The withdrawal of consent does not affect the legality of the data processing to which the consent was given prior to the withdrawal.

The withdrawal of consent shall be expressed in a format that can be printed and/or reproduced in writing, including in electronic or verifiable formats.

Upon receipt of the data subject's request for withdrawal of consent, the data controller and/or the data controller-cum-processor shall notify the data subject of possible consequences and damage upon withdrawal of consent.

Following the implementation of withdrawal, the data controller, data processor, data controller-cum-processor, and the third party must cease and request relevant organizations and/or individuals to cease the processing of the data to which the consent has been withdrawn by the data subject. However, the regulations do not specify any period after the notification of the consequences and damage of the withdrawal and before ceasing the processing so the data controllers must stop processing the data as soon as they complete the notification obligation.

Right to Data Deletion [62]

The right to delete personal data shall apply in the following cases:

- The data subjects have found that the data is no longer necessary for the purpose(s) consented and accept possible damage upon requesting for data deletion;
- Withdrawal of consent;
- There is an objection to the data processing and the data controller or the data controller-cum-processor has no legitimate reason to continue the processing;

- The personal data processing is not for the consented purpose(s) or is in violation of the law;
- The personal data shall be deleted in accordance with the law.

However, there are exceptions to the exercise of this right which include:

- The deletion of data is not permitted by law;
- The personal data is processed by a competent state agency for the operation of the state agency in accordance with the law;
- The personal data has been made public in accordance with the law;
- The personal data is processed to serve legal requirements, scientific research and statistics in accordance with the law;
- A state of emergency has been proclaimed on the national defense, national security, social order and safety, major disasters, and dangerous epidemics; there are dangers threatening the national security and defense but not to the extent of proclaiming the state of emergency; in order to prevent and fight against riots and terrorism, to prevent and fight against crimes and legal violations;
- It is required to respond to an emergency threatening the life, health or safety of the data subject or other individual(s).

There are also cases where the personal data must be deleted, regardless of the requests of the data subject:

- The data has been processed for improper purposes or the purpose(s) consented by the data subjects for the data processing has been fulfilled;
- The storage of personal data is no longer necessary for the operation of the data controller, data controller-cum-processor, data processor, and third party;
- The data controller, data controller-cum-processor, data processor, or third party is dissolved or no longer operates or declares bankruptcy or has its business operations terminated in accordance with the law.

This is a straightforward version of the right to deletion where the data would simply be deleted and does not include the right to be delisted/right to be forgotten such as under the GDPR.[63]

Right to Provision of Data (data portability) [64]

The data controller and data controller-cum-processor are entitled to:

- Provide the data subject's personal data to other organizations and/or individuals with the consent of the data subject, unless otherwise provided by law;
- Provide, on behalf of the data subject, the data subject's personal data to other organizations and/or individuals under the consent of the data subjects to such representation and authorization, unless otherwise provided by law.

However, the right might not be exercised in the following cases:

- The national defense, security, and/or social order and safety may be compromised;
- The provision of personal data of the data subject may affect the safety, physical or mental health of others;
- The data subject does not agree to provide or give consent for representation or authorization to receive his/her personal data.

Right to Restrict Processing [65]

Data subjects may request to limit the processing of their personal data unless otherwise provided by the law. However, in the rest of the PDPD, there is no other mention of this right, and without further guidance or instructions, the procedures, consequences, and implications of the exercise of this right remain unclear.

Right to Object to Processing [66]

Data subjects may object to the processing of their personal data by the data controller or data controller-cum-processor to prevent or limit the disclosure of their personal data or the use of their personal data for advertising or marketing purposes unless otherwise provided by law.

Miscellaneous Rights

Data subjects also have the right to file complaints, denunciations and lawsuits pursuant to the law,[67] the right to seek compensation for damages due to violations of their personal data,[68] and the right to defend themselves pursuant to the Vietnamese Civil Code.[69] However, due to these being statutory rights that are only mentioned in the PDPD, the Handbook will not delve further into them.

Time Limit for Exercising the Rights

Most of the data subject rights mentioned above have a time limit for fulfillment of 72 hours such as the Right to Provision, Right to Correction, Right to Deletion, Right to Restriction, and Right to Object, while the remaining rights do not have a clear deadline. This is a considerably narrower time frame when compared to other data protection legislation such as the EU's GDPR which allows for one month to respond to the data subject's requests. [70]

Data Protection Officer

Regarding sensitive personal data processing, from the commencement and throughout the sensitive personal data processing, businesses, and organizations need to implement measures for personal data protection, including designating a personal data protection department or DPO (MPS opined that the DPO position can be outsourced to a non-employee individual). It means that the designation will be mandatory from July 1, 2023 for organizations and businesses with activities related to sensitive personal data.

Micro-enterprises, small enterprises, medium-sized enterprises, and start-up enterprises (except for enterprises directly engaged in personal data processing) shall be entitled to choose to be exempt from this obligation for the first 02 years from the date of establishment.[71] Therefore, if a small business was established in 2020, it must still appoint a DPO as soon as the PDPD takes effect. Additionally, Article 24 of the PDPD and the data protection impact assessment form still require businesses to provide information about this position. As a result, this exemption appears to have little practical significance.

Interestingly, the processing of sensitive personal data is a basis for appointing a DPO. However, the PDPD does not provide specific regulations on the DPO's responsibilities regarding the protection of sensitive personal data. The PDPD also does not clearly define the roles and duties of the DPO, primarily positioning this role as a point of contact with the authorities. As a result, each business interprets the DPO's roles differently, sometimes leading to conflicts of interest. In addition, there is currently no regulation on the requirements of a DPO, however, it could be surmised that the DPO must be a qualified individual with experience and knowledge regarding personal data protection. This matter is further addressed in the first draft of the Personal Data Protection Law and will be mentioned in the following section of this Handbook.

Engaging Personal Data Processors

When engaging a data processor, the data controller must make a proper selection of the data processor with express task assignments and only work with a data processor that has in place appropriate security measures.[72] It is recommended that the controller has a set of standards regarding data protection, compliance, security, etc. to select the most appropriate processors.

It is also mandatory that upon engaging a data processor, the data controller must enter into a data processing agreement with the data processor. The data processor shall in turn receive personal data only after having signed a contract or agreement on data processing with the data controller and process the personal data in accordance with the contract or agreement signed with the data controller.[73] The data processor must also delete and/or return all personal data to the data controller after the completion of the data processing.[74]

In addition, the processor is responsible for assisting the controller in demonstrating compliance with personal data protection regulations. As a result, in practice, the contractual obligations imposed on the processor are often designed to be similar to those of the controller, such as maintaining data processing logs, coordinating responses to regulatory inquiries, and implementing appropriate organizational and technical measures (TOMs), etc.

Enforcement and Sanctions

Supervisory Authority

Personal data/information in different sectors will be regulated by their own specialized bodies pursuant to sector-specific regulations such as in labor, consumer rights protection, cybersecurity, etc. The only body that is officially designated as being in charge of personal data protection is the A05 which is responsible for helping the MPS to carry out state management of personal data protection.[75] A05 will be responsible for and act as the point of contact for many administrative procedures regarding personal data such as notifying personal data breaches, receiving dossiers, forms, and information on personal data protection such as personal data processing impact assessment dossiers, data protection officer information notification, inspecting, examining, handling complaints and denunciations, and addressing violations of regulations on personal data protection in accordance with the law.

Current Enforcement and Sanctions

Currently, on administrative sanctions, Decree No. 15/2020/ND-CP on penalties for administrative violations in the fields of post, telecommunications, radio frequency, IT, cybersecurity, and electronic transactions (as amended and supplemented by Decree No. 14/2022/ND-CP) is the primary legal documents pertaining to sanctions against personal information violations.

Under this Decree, violations related to personal data (referred to as "personal information" in these regulations) are subject to the following penalties:[76]

- A fine ranging from VND 10 million to VND 30 million for unauthorized collection, use, or sharing of personal information, along with a mandatory remedy requiring the deletion of personal information obtained through the violation.
- A fine ranging from VND 10 million to VND 50 million for failure to update, amend, or delete personal information as required by law.
- A fine ranging from VND 10 million to VND 70 million for failure to comply with security standards or failure to address cybersecurity incidents, with an additional mandatory remedy requiring the implementation of appropriate cybersecurity measures if not correctly applied.

Regarding the field of consumers' rights protection, Article 46 of Decree No. 98/2020/ND-CP (as amended by Decree No. 24/2025/ND-CP) outlines specific fines for violations concerning consumers' information, including personal data.

These fines range from VND 20,000,000 to VND 30,000,000 and apply to the following infractions:

- Engaging a personal data processor without consumer consent or failing to establish a formal authorization/contract specifying the responsibilities of both parties.
- Failing to fulfill or inadequately implementing the consumer's right to be informed about data processing activities.
- Collecting or using consumer information without proper consent or inaccurately/inconsistently with the declared purpose and scope.
- Failure to comply with consumer requests regarding the review, correction, update, deletion, transfer, or cessation of data processing.
- Failure to delete consumer information after the retention period expires, as required by the applicable consumer data protection regulations or legal provisions.

Similarly, fines ranging from VND 30,000,000 to VND 40,000,000 are imposed for the following violations:

- Failure to receive, process, or respond to consumer complaints, requests, or inquiries related to data processing activities.
- Failure to notify competent authorities of data system incidents within the required timeframe.
- Lack of appropriate security and safety measures when collecting, storing, or using consumer information, or failure to implement preventive measures against data security violations.
- Unauthorized transfer of consumer information to third parties without obtaining the consumer's consent as required by law.

Notably, if the violation is committed by an organization or involves sensitive personal data, the applicable fine is doubled; meanwhile, where the violation is carried out by a large-scale digital platform operator, the fine is increased fourfold.

Under the PDPD, there are also measures that the MPS can take, such as requesting the party performing the cross-border data transfer to cease the cross-border transfer of personal data in cases where:

- It is detected that the transferred personal data is used for activities that violate the interests and national security of the Socialist Republic of Vietnam;
- The cross-border data transferrer fails to comply with the provisions regarding the cross-border data transfer impact assessment;
- The personal data of Vietnamese citizens is disclosed or lost.[77]

There are also criminal sanctions against individuals in violation of personal information. According to Article 288 of the Criminal Code 2015 (amended in 2017), depending on the severity of the violation, an individual can face fines of up VND 01 billion or up to 07 years in jail for buying, selling, exchanging, giving, amending, altering, or disclosing the lawful private information of an agency, organization, or individual on computer networks or telecommunications networks without the permission of the information's owner.

Draft Document on Enforcement and Sanctions

While the PDPD was issued back in 2023, the sanctions for violations of the PDPD are still in the drafting phase and have not been officially issued. This section will detail the sanctions prescribed in the Draft Decree on Administrative Sanctions for Cyber-security Violations publicized in May 2024 ("**Draft Decree**").

The Draft Decree stipulates various violations including violations of the obligations that organizations and individuals must comply with under the PDPD when processing personal data in Vietnam and/or of Vietnamese citizens, including violations of personal data protection regulations, failure to ensure the exercise of data subjects' rights or failure to establish appropriate data protection management measures when performing sensitive personal data processing activities, etc.

According to the Draft Decree, violations of personal data protection may be subject to fines of up to VND 100 million (in cases with severe consequences, the penalty could be up to five times this amount) or 5% of the total revenue of the previous fiscal year in Vietnam for individuals (for organizations or enterprises, the penalties are doubled). In addition, there are also supplementary penalties that could significantly impact the data processing activities and business activities, such as: (1) revocation of the business license for the line of business requiring the collection of personal data for a period of 01 to 03 months; and (2) temporary suspension or suspension of personal data processing for a period of 01 to 03 months.

These penalties apply to most of the compliance obligations under the PDPD as analyzed above, including penalties for: (1) Violations of personal data protection principles; (2) Violations of data subject rights (e.g., failure to obtain consent, failure to notify data subjects about processing activities, or failure to comply with requests to provide, modify, or delete personal data, etc.); (3) Violations of regulations on unauthorized collection, transfer, purchase, or sale of personal data; (4) Violations of procedural requirements (e.g., failure to notify data protection breaches, failure to prepare DPIA and DTIA dossiers), or failure to notify A05 when transferring personal data overseas); and (5) Violations of regulations on personal data protection measures, etc.

Nevertheless, it is evident that the Draft Decree still contains contradictions and overlaps. Hopefully, in future drafts, these issues will be thoroughly addressed before the decree is officially issued.

Privacy Compliance

DRAFT

PERSONAL DATA PROTECTION LAW

As briefly touched on at the beginning of this Handbook, in September 2024, the MPS publicized the first draft of the Personal Data Protection Law in order to expand and solidify the regulations regarding personal data protection, and on 10 March 2025, the latest version was released ("**Draft Law**"). The Draft Law has made some modifications and changes compared to the PDPD, the most prominent of which will be detailed in this section.

New Definitions

- Personal data now includes all forms of personal data, not just electronic data.[78]
- Data on land users, land data containing information of land users, data on salary, benefits, and other incomes have been added as sensitive personal data.[79]
- Customer identification information, account information of customers of credit institutions, foreign bank branches, and payment intermediary service providers are no longer considered sensitive personal data.[80]
- Personal Data Protection Organization is an organization certified by the specialized authority for personal data protection and designated by the Controller, the Controller-cum-Processor, the Third Party, the Party transferring personal data abroad, the Party receiving data of Vietnamese citizens as the personal data protection department.[81]
- Personal Data Protection Expert is a person appointed by the Controller, the Controller-cum-Processor, the Third Party, the Party transferring personal data abroad, the Party receiving personal data of Vietnamese citizens as a personal data protection officer, with sufficient capacity to protect personal data.[82]

Administrative Fines

The administrative fines have been confirmed to range from 1% to 5% of the revenue of the previous year of the violating organization, or enterprise.[83] This is a huge development and could signify that the government is very serious about protecting personal data.

Rights of the Data Subject

- The right to restrict data processing has been elaborated. It is stated that data subjects have the right to request the restriction of processing of their personal data if there are doubts about the accuracy of the data. However, there is still no further regulation on the consequences or the method of performing this right.[84]
- The right to object can now be invoked for any reason, instead of to prevent the disclosure of personal data or prevent the use of the data for marketing purposes.[85]

Processing Activities

- New personal data processing activities such as analysis, compilation, publication, encryption, decryption, etc. have been added, similar to those prescribed in the Data Law 2024.[86]
- Sensitive personal data when stored, transferred, received, or shared in cyberspace must now be encrypted.[87]

Processing Children's Data

- The age range of children where personal data processing requires consent from both the child and the legal representative has been updated to range from 07 to under 15 years of age.[88]
- Where given, children can now withdraw their consent instead of only the legal representative.[89]

Marketing, Targeted Advertisement

- The collection of data through website and application monitoring can only be conducted with the consent of the data subjects – meaning that the use of cookies has been specifically called out as needing consent to be implemented.[90]
- User must now be given an option to refuse marketing information.[91]
- Hiring another organization to perform marketing business, behavioral or targeted advertising services on behalf of the company based on its customers' personal data is now prohibited.[92]

Big Data

Article 26 of the Draft law details the data protection measures when processing big data such as: applying encryption at rest and during transit, employing powerful authentication and access control methods, data pseudonymization, data anonymization, constant monitoring, routine audit, data security training, establishing binding mechanisms with partners and suppliers, etc.

Artificial Intelligence, blockchain and metaverse

- Article 27(1) of the Draft Law stipulated that organizations and individuals are entitled to use personal data to research and develop self-learning algorithms, artificial intelligence and other automated systems in compliance with legal regulations. Article 27(2) also stipulates that the organization or individual must inform data subjects about the automated processing of personal data, explain the impact of algorithms, artificial intelligence and automated systems on the rights and legitimate interests of data subjects, and provide options for data subjects to have the right to opt-out.
- Article 27(3) also establishes personal data protection measures to be applied in artificial intelligence, blockchain and metaverse such as: establishing control mechanisms, protecting personal data according to the highest international standards, implementing transparent AI monitoring and control mechanisms, developing an AI impact assessment system, etc.

Cloud Computing

Another edition in the Draft Law is the inclusion of the mandatory contents of the data processing agreement with cloud service providers, in which the agreement must:[93]

- Clearly state in the contract and agreement on compliance with the provisions of Vietnamese law on personal data protection; provide information about the department and personnel protecting personal data in case of processing sensitive personal data; comply with the provisions on personal data protection administrative procedures according to the provisions of law;
- Only process customer data for the benefit and on behalf of the customer;
- Have requirements on security, technical, organizational measures and clearly state them in the contract;
- Immediately notify any changes that may affect personal data;
- Compensate for damages (if any);
- Provide reasonable audit reports, delete customer data upon request;
- Fully implement technical measures to ensure that access to data is reasonably decentralized.

In reality, most of the popular cloud computing service providers in the world today are global technology corporations such as Amazon, Google, Microsoft, IBM, etc. These parties all have their own contract templates and it will be very difficult for Vietnamese individuals and organizations to negotiate to change or add any clause, even the smallest one. Moreover, these contract templates do not allow for the choice of applicable law but will determine the law of a country/territory outside of Vietnam. This provision could cause much disruption to the operations of cloud service users and providers.

Labor

Although the PDPD and the current labor laws do not have specific regulations, Article 29 of the Draft Law provides considerations regarding the processing of personal data for recruiting the workforce and monitoring employee performance. Namely, data collected during the recruitment process has to be publicly required as in Article 16 of the Labor Code;[94] or already stated in the employee's personnel file. Processing of such data must be done in accordance with the applicable law, such as seeking consent, or following allowed storage periods.

In case of foreign employers hiring Vietnamese employees (residing in Vietnam) to work at companies overseas, the employers shall be mandated to sign an extra contract with the investing firm in Vietnam properly accepting personal data processing with the details regulating the processing of personal data for employees. Additionally, the investing company must be provided with a copy of the employee's personal data preserved for archival purposes.

In addition, the following requirements are mandated for employers who use technological or technical measures to monitor employees:

- Ensure the employees are aware of the relevant technological and technical measures.
- Request the employee's consent to monitoring via technological and technical means.
- Include information on the application of monitoring measures and contents in the personal data processing impact assessment.
- Commit to refraining from using technologies, technical solutions, and monitoring methods that are prohibited by law.

The aforementioned provisions constitute new regulations governing the processing of personal data in employment relationships, aiming to enhance the protection of employees' rights and interests as data subjects.

Banking, Financial and Credit

In the Draft Law, it is prescribed that financial, banking, credit and credit information institutions:[95]

- Must not buy, sell credit information or illegally transfer credit information between financial, credit and credit information institutions;
- Fully apply regulations on the protection of sensitive personal data, payment, credit, and credit information security standards as prescribed by law;
- Must not use credit information of data subjects to score credit, assess credit information, and assess creditworthiness of data subjects without the consent of data subjects;
- The results of credit information assessment of data subjects to be used in business relationships with another party must only be in the form of Pass or Fail, Yes or No, True or False, or on a scale based on the data that financial, banking, credit and credit information institutions collect directly from customers;
- Clearly identify and state the stages where personal data de-identification measures must be applied;
- Data subjects must be notified of incidents and loss of bank account, financial, and credit information.

Contracts with Data Subjects

Article 32 of the Draft Law states that contracts and agreements with data subjects must include provisions related to personal data protection. These provisions should clearly specify the responsibilities, rights, and obligations that all parties involved are required to comply with.

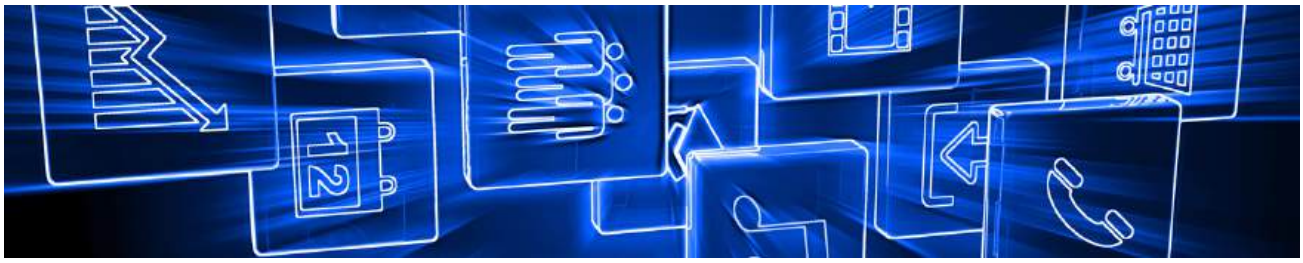
Location Data

Article 33 of the Draft Law mandates that tracking through Radio Frequency Identification (RFID) tags and other technologies should not be applied unless there is explicit consent from the data subject or a legal requirement. Also, mobile application platforms must clearly inform customers and users about the use of location data, implement measures to prevent the collection of location data by unrelated organizations or individuals and provide options for users regarding location tracking.

Social Media, Online Media Service

The Draft Law also has provisions regarding social media services[96] – defined as platforms that allow users to create profiles, share content, and interact with others; send text messages, images, and videos, and make calls over the Internet; make video calls between devices; platforms and services that allow players to participate in games over the Internet; and organize online meetings, seminars, and classes; and online media services[97] – defined as platforms that deliver video content such as movies, television shows, and short videos over the Internet; platforms that allow users to listen to music online; services that allow live streaming of video content to viewers in real-time. Article 34(3) stipulates that organizations and individuals providing social networking services and online media services are responsible for

- Protecting personal data of Vietnamese citizens when operating in the Vietnamese market or appearing on mobile application stores provided to the Vietnamese market.
- Clearly announcing the content of personal data collected when data subjects install and use social networks and online media services. Must not illegally collect personal data and do not collect data outside the scope of the agreement with customers.
- Do not request photos or videos that contain parts of or the entire citizen identification cards or identity cards as a factor in account authentication.
- Providing options allowing users to refuse the collection and sharing of cookies.
- Providing a "do not track" option or only track social networking and online media service usage activities with the user's consent.
- Notifying in a specific, clear, written manner the sharing of personal data as well as the application of security measures when conducting advertising and marketing activities based on customers' personal data.
- Eavesdropping, wiretapping or recording calls and reading text messages without the consent of the data subject are prohibited;
- Publishing a privacy policy that clearly explains how personal data is collected, used and shared; providing users with the right to access, edit, delete data and set privacy for personal information; protecting the personal data of Vietnamese citizens when transferred outside the territory of Vietnam; establishing a mechanism for users to report violations of personal data protection; developing a process for handling violations of personal data protection quickly and effectively;
- Notifying data subjects of incidents and violations of regulations on personal data protection of social network accounts and online media services within 72 hours of the occurrence of the violation or incident, along with the results of handling, overcoming the consequences, assessing the severity of the incident and potential risks arising.



Personal data registered for social network accounts and online media services is not subject to processing without the consent of the data subject.[98]

Biometric Data

According to Article 35 of the Draft Law, organizations and individuals that collect and process biometric data must fully comply with the legal provisions on personal data protection, have in place physical security measures to protect its storage and transit devices, apply strong encryption during data transit, have an access limitation and monitoring system and comply with relevant international standards. They must also clearly inform data subjects about the potential consequences and risks associated with the collection and processing of biometric data

Personal Data Protection Organizations

Personal Data Protection Organizations to provide services must have experts with Certificates in Capacity for Personal Data Protection, be registered in the business fields of legal and technology or legal, technology consultancy, and have a minimum personal data credit rating of "Trusted". The organization must apply and be approved by the competent authority on personal data protection before it can provide services. [99]

Personal Data Protection Experts

Personal Data Protection Experts must have college-level degrees and Certificates in Legal and/or Technical Capacity for Personal Data Protection issued by an organization approved by the competent authority on personal data protection. [100]

Personal Data Protection Credit Rating

The personal data protection credit level is rated by organizations approved by the competent authority on personal data protection to provide the service. The credit rating method must assess the risk factors (market, technology, personnel, financial risks, etc.) and the extent of their impact on the ability to fully and properly fulfill the obligations regarding personal data protection. There are three credit levels: "Highly Trusted"; "Trusted"; and "Not Trusted". [101]

Personal Data Processing Service Providers

According to Article 44(1) of the Draft Law, personal data processing services are now defined to include: (i) Personal data analysis and aggregation services; (ii) Credit rating services based on personal data; (iii) Online personal data collection services from websites, mobile applications and social networks and offline personal data collection services from physical sources such as surveys, applications and data from offline devices; (iv) Personal data analysis and exploitation services, including: using analytical tools to search for information, trends and patterns from personal data; applying data mining methods to extract value from personal data, predict customer behavior or optimize services; (v) Personal data encryption services during transmission and storage; (vi) Personal data processing services by the Data Processor on behalf of the Controller, the Data Controller-cum-Processor. There will be specific conditions, and procedures for applying for a business license to operate in these fields, which will be determined by the government.[102]

DPIA and DTIA Dossiers

The DPIA and DTIA Dossiers must now be updated once every six (06) months when there are changes. Cases, where an immediate update is required, include (i) When the company dissolves or merges;(ii) When there is a change in information regarding the Personal Data Protection Organization and the Personal Data Protection Expert; (iii) When a new business sector or service is introduced, or when the business stops offering services or products related to personal data that were registered in the DPIA or DTIA dossiers.[103] Furthermore, state agencies are now exempt from conducting an impact assessment for processing and transferring personal data abroad, excluding public service entities and state-owned enterprises. [104]

Personal Data Protection

The Draft Law requires the appointment of a PDPO and/or PDPE and the communication of their information to the competent personal data protection authority as a measure for protecting basic personal data.[105] Meaning all organizations involved in the processing of personal data will have to comply with this obligation. However, state agencies are exempted from this obligation, with the exception of public service entities or state-owned enterprises.[106]

Within 01 year from the effective date of the Law, agencies, organizations and enterprises may designate departments and personnel with the function of protecting personal data in place of the PDPO and PDPE to ensure the implementation of regulations on personal data protection.[107] Furthermore, small enterprises and startups have the right to choose to be exempt from the requirement for a PDPO/PDPE during the first five years of the company's establishment. However, this exemption does not apply to small enterprises or startups that directly engage in activities involving the processing of personal data.[108]

Personal Data Protection Audit [109]

The personal data protection audit is carried out regularly, periodically, or unexpectedly in the following cases (i) When there is a violation of the laws on personal data protection; (ii) To perform state management tasks as required by law.

Entities that may be subject to the audit include:

- Agencies, organizations, and individuals involved in personal data processing;
- Organizations and individuals engaged in business activities related to personal data processing;
- Organizations and individuals required to perform DPIA and DTIA;
- Organizations certifying personal data protection capacity.

The content of the personal data protection audit includes:

- The current state of compliance with personal data protection;
- Activities related to the impact assessment of personal data processing and the impact assessment of transferring personal data abroad;
- Activities to certify the required technological and legal capabilities for personal data protection.

The competent authority on personal data protection will issue an inspection decision and notify the audited entity at least 15 working days in advance regarding the time, content, and members of the inspection team.

The audited entity must prepare all relevant materials as required by law. The results of the audit will be kept confidential in accordance with legal provisions.

Privacy Compliance

PROCESSING PERSONAL DATA
IN SPECIFIC SECTORS

Processing personal data across sectors such as banking and finance, cyberspace, labor, consumer rights protection, and information security involves sector-specific regulations and practices to safeguard privacy and ensure compliance

Banking, Financial and Credit

"Customer information of credit institutions and foreign bank branches must be kept confidential and only provided in accordance with the provisions of the Law on Credit Institutions"

Clause 1, Article 4 of Decree No. 117/2018/ND-CP ("**Decree 117/2018/ND-CP**")

Customer information in this case is information provided by customers, information arising during the process of customers requesting or being provided by credit institutions with banking operations, products, and services in permitted activities, such as information on the identity of the client, the account, the assets, transactions, etc.

From the perspective of banking law, according to the provisions of Clause 2 and Clause 3, Article 13 of the Law on Credit Institutions 2024, credit institutions are obliged to:

- ensure the confidentiality of customer information of credit institutions and foreign bank branches according to Government regulations;
- not provide customer information of credit institutions and foreign bank branches to other organizations and individuals, except in cases where there is a request from a competent state agency according to the provisions of law or with the consent of the customer.

Article 14 of Decree 117/2018/ND-CP has more specific regulations on this issue as follows: Credit institutions have the right to refuse to provide customer information to state agencies, other organizations, and individuals for requests to provide customer information that are not in accordance with the provisions of law, or requests to provide duplicate customer information, or not within the scope of customer information that credit institutions and foreign bank branches are storing according to the provisions of law.

Credit institutions are responsible for:

- Ensuring the safety and confidentiality of customer information during the process of providing, managing, using, and storing customer information;
- Resolving customer complaints regarding the provision of customer information according to the provisions of law;
- Organizing supervision, inspection, and handling of violations of internal regulations on keeping confidential, storing, and providing customer information.

At the same time, credit institutions are responsible for refusing to investigate, freeze, detain, or transfer customer deposits, except in cases where there is a request from a competent state agency as prescribed by law or with the customer's consent.

On the other hand, according to Clause 2, Article 4 of Decree 117/2018/ND-CP, credit institutions are not allowed to provide customer authentication information when accessing banking services, including secret codes, biometric data, customer access passwords, and other customer authentication information to any agency, organization, or individual, except in cases where there is written consent from that customer or in other forms as agreed with that customer.

Credit institutions must issue internal regulations on keeping confidential, storing, and providing customer information and organize consistent implementation within the credit institution. Internal regulations on keeping confidential, storing and providing customer information must include at least the following contents:

- Processes and procedures for receiving, processing and providing customer information; processes and procedures for storing and protecting the confidentiality of customer information;
- Monitoring, inspection and handling of violations of internal regulations on keeping confidential, storing and providing customer information;
- Decentralization of authority, power and obligations of units and individuals in keeping confidential, storing and providing customer information.

Not only credit institutions, in banking activities, payment intermediary service providers are also responsible for keeping confidential information related to account holders, transactions and balances on payment accounts of their service users, except where otherwise provided by law. Payment service providers and payment intermediary service providers have the right to refuse requests from other organizations and individuals to provide information related to accounts, transactions and balances on accounts, e-wallets, transactions and balances on e-wallets, except where required by competent state agencies as prescribed by law or with the consent of customers.

Recently, in an attempt to ensure the security for online banking services, the State Bank of Vietnam has issued Circular No. 50/2024/TT-NHNN to impose some new obligations, which shall come into effect from January 01, 2025,[110] on credit institutions and foreign bank branches when providing online banking services.
In summary, the new requirements are as follows:

- **High-Level Security**: The online banking system must adhere to security standards, (equivalent to Level 3 requirements (for general systems) and Level 4 requirements (for financial transaction switching and electronic clearing systems), as outlined in TCVN 11930:2017 and other regulations of the State Bank of Vietnam.
- **Customer Data Protection**: The confidentiality and integrity of customer information, as well as the system's availability must be guaranteed to provide uninterrupted services.
- **Transaction Management**: Transaction must be classified and risk assessment carried out based on customer factors, transaction types, and limits, in order to select and implement suitable authentication methods (e.g., OTP, biometric authentication) in compliance with regulatory requirements.
- **Regular Security Assessments**: Conduct annual security assessments to identify and address vulnerabilities.
- **Risk Management**: Identify, assess, and mitigate potential risks to ensure secure operations.
- **Technology Infrastructure**: Utilize licensed hardware and software with clear origins. Implement timely upgrades and replacements to address security vulnerabilities.
- **Operational Compliance**: The Online Banking system must operate in full compliance with all relevant laws and regulations.

Moreover, in order to ensure transparency, credit institutions and foreign bank branches will be mandated to inform clients about terms of the agreement on the provision and use of online banking services, including the content of the personal data processing for online banking services, including (i) types of client data that the unit collects, (ii) purposes of using client data; (iii) the unit's responsibility for ensuring the confidentiality of client data in accordance with the law, except where the unit and the client have reached another agreement on the protection of client data in accordance with law.

Consumers' Rights Protection

According to the Law on Consumers' Rights Protection 2023, traders who process consumers' information, either by themselves or via a third party, must protect such information in accordance with the laws. Processing consumers' information via a third party will require the consent of the consumers.[111] In this case, consumer information includes consumers' personal information, information about the process of purchasing and using products, goods and services of consumers and other information related to transactions between consumers and business organizations and individuals.[112]

Unless otherwise provided by law, organizations and individuals engaged in business must collect, store, and use consumer information in accordance with established rules for protecting consumer information. These rules must include the following contents:

- The purpose of collecting information;
- The scope of information usage;
- The duration of information storage;
- Measures to protect information and ensure the security of consumer information.

Business organizations and individuals must publicly disclose the information by posting it in a visible location at their headquarters, business locations, and on their websites or applications (if applicable), ensuring that consumers can access it before or at the time of information collection. [113]

Trading organizations and individuals must notify consumers clearly, publicly, and in a suitable form about the purposes, scope of collecting and using information, storage period of consumers' information before carrying on and must obtain the consent of the consumers, except in the case of collecting information that has been made public by the consumers or other cases as prescribed by law.[114]

Trading organizations and individuals are responsible for establishing a mechanism for consumers to choose the scope of information to provide and express their agreement or disagreement, except in the case of collecting information that has been made public by the consumers or selling and providing products, goods, or services as requested by consumers and within the scope of the information agreed upon by the consumers, or to perform legal obligations.[115] Before changing the purposes or scope of information use notified to consumers, trading organizations, and individuals must re-notify and obtain consumers' consent to the change.

Trading organizations and individuals are obliged to use consumers' information accurately, in accordance with the notified purposes and scope, and must obtain the consent of the consumers, except in the following cases:[116]

- Having a separate agreement with consumers on the purposes and scope of use other than the notified purposes and scope;
- In order to sell and provide products, goods and services at the request of consumers and only within the scope of information agreed by consumers;
- In order to perform obligations according to the provisions of laws.

Trading organizations and individuals collecting and using consumers' information must have a mechanism for consumers to choose whether or not to allow the following acts:[117]

- Sharing, disclosing, and transferring information to third parties, except in cases where trading organizations or individuals transfer information that has been collected in accordance with laws to a third party for storage or analysis to serve the transferor's business activities and both parties have a written agreement that the third party is responsible for protecting consumers' information according to regulations;

- Using consumers' information to advertise and introduce products, goods, services and other commercial activities.

Business organizations and individuals must ensure the safety and security of consumer information that they collect, store, and use, and implement measures to prevent the following actions (i) Theft or unauthorized access to information; (ii) Unauthorized use of information; (iii) Unauthorized modification, updating, or deletion of information.[118] When there are feedback, requests, or complaints from consumers related to information being illegally collected or used for the wrong purposes or outside the scope as notified, trading organizations and individuals must receive and resolve the issue quickly and timely.[119]

Consumers have the right to request trading organizations and individuals to inspect, modify, update, destroy, transfer, or stop transferring their information to third parties. Trading organizations and individuals are responsible for performing the above requirements or providing consumers with tools and information to perform such actions themselves according to the provisions of laws. [120]

Trading organizations and individuals must destroy consumer information at the end of the storage period as prescribed in their consumers' information protection principles or other relevant laws.[121]

In the context of consumer rights protection, organizations (data controllers or processors) or data storage providers (processors engaged in data storage activities) are required to notify the competent state authority of any system intrusion that poses a risk to the security and safety of consumer information. The notification deadline for such incidents is shorter compared to that of the PDPD, at 24 hours from the time of detection.

However, the regulations do not provide a specific definition or criteria for determining a *"risk to the security and safety of consumer information"*, leaving it to organizations to make this assessment.

Information Technology

According to Article 22(2) of the Law on Information Technology 2006, the processors of personal information in the cyberspace shall be obligated to:

- Notify the person of the form, scope, location and purpose of the collection, processing and use of that person's personal information;
- Use the collected personal information for the right purposes and only store such information for a certain period of time as prescribed by law or as agreed between the two parties;
- Take necessary management and technical measures to ensure that personal information is not lost, stolen, disclosed, changed or destroyed;
- Immediately take necessary measures upon receiving a request to re-check, correct or cancel the information; do not provide or use relevant personal information until such information is corrected.

Labor

Fundamentally, employees are considered data subjects and covered by data protection regulations like any other individual. On the other hand, the imbalance of power characterizes the employment relationship, with employees usually being in the weaker role, the law typically imposes stricter requirements to safeguard the interests of this vulnerable group. However, currently, the PDPD does not have not any specific provisions pertaining to personal data processing in in the field of labor. The Labor Code 2019 only has one regulation regarding data which states that employees must provide truthful information to employers regarding their full name, date of birth, gender, place of residence, educational qualifications, professional skills, health certification, and other matters directly related to the conclusion of the labor contract as requested by the employer.[122] As such, it would seem that until the Draft Law comes into effect, the processing of personal data of employees will only have to comply with the general regulations regarding personal data processing prescribed in the PDPD.

Cyberspace

Organizations and individuals that process personal information have the responsibility to protect such information and shall make public the personal data processing, protection measures.

The personal information subject has the right to request the organization or individual processing personal information to provide his/her personal information that the organization or individual has collected and stored.[123] The personal information subject also has the right to request the organization or individual processing personal information to update, amend, cancel his/her personal information that the organization or individual has collected and stored or to stop providing his/her personal information to a third party. [124]

Article 17(1) of the Law on Cyberinformation Security 2015 states that organizations and individuals processing personal information shall have the following responsibilities:

Collect	Use	Share
Collect personal information after obtaining the consent of the subject of personal information regarding the scope and purpose of collecting and using such information	Only use the collected personal information for purposes other than the original purpose after obtaining the consent of the subject of personal information	Not provide, share, or disseminate personal information that they have collected, accessed, or controlled to third parties, except with the consent of the subject of such personal information or at the request of a competent state agency

Immediately upon receiving the request of the personal information subject to update, amend, cancel personal information or request to stop providing personal information to a third party, the personal information processing organization or individual shall: [125]

- Implement the request and notify the personal information subject or provide the personal information subject with access to update, amend, cancel his/her personal information;

- Apply appropriate measures to protect personal information; notify the subject of that personal information in case the request cannot be fulfilled due to technical or other factors.

Organizations and individuals processing personal information must destroy stored personal information when the purpose of use has been completed or the storage period has expired and notify the subject of personal information, except in cases where the law provides otherwise.[126]

Organizations and individuals processing personal information must apply appropriate management and technical measures to protect the personal information they collect and store; and comply with technical standards and regulations on ensuring network information security.

When a network information security incident occurs or is at risk of occurring, organizations and individuals processing personal information must apply remedial and preventive measures as soon as possible[127]

Specifically, Circular No. 20/2017/TT-BTTTT requires organizations and individuals operating information systems to:

- Monitor and report: Proactively monitor systems to detect incidents. Upon detection, detailed records must be kept and notifications or reports must be submitted as required.
- Verify and coordinate: Upon receiving a notification, organizations must promptly respond to confirm the information. Subsequently, they must collaborate with relevant entities, such as cybersecurity units, incident response teams, and internet service providers, to analyze, assess, and verify the incident.
- Incident response: Implement initial incident response measures according to approved plans or procedures outlined in the Circular.

In addition, the Law on Cybersecurity also imposes obligations on service providers in cyberspace to make a response plan in case of leak or loss of data or risk thereof, as well as to inform the incident to users and the professional cybersecurity force as prescribed by the law.[128]

Privacy Compliance

CERTIFICATIONS &
PERSONAL DATA PROTECTION MEASURES

Personal data protection is not only an obligation under the laws, it is becoming more and more important given the increasing value of personal data. Businesses are adopting comprehensive data protection protocols to ensure data confidentiality, integrity, and availability.

Personal Data Protection Measures

Requirements under PDPD

The data controllers and processors shall implement measures to protect personal data throughout the processing of personal data. Such measures include:[129]

- Management measures taken by organizations and/or individuals in relation to personal data processing;
- Technical measures taken by organizations and/or individuals in relation to personal data processing;
- Measures taken by competent state management agencies in accordance with the PDPD and relevant laws;
- Investigation and procedural measures taken by competent state agencies;
- Other measures as prescribed by law.

When processing basic personal data, aside from the aforementioned measures, the following measures must also be taken:[130]

- Developing and promulgating the regulations on personal data protection, specifying the tasks to be completed in accordance with the PDPD;
- Encouraging the application of standards for personal data protection appropriate to the fields, industries and activities in relation to personal data processing;
- Checking the systems, facilities and equipment serving the personal data processing for network security before the processing, permanent deletion or destruction of devices containing personal data.

When processing sensitive personal data, all aforementioned measures are required in addition to:[131]

- Designating a department with the function of personal data protection, appointing personnel in charge of personal data protection;
- Notifying the data subjects that their sensitive personal data shall be processed, except for the cases specified in Clause 4 Article 13, Article 17, and Article 18 of the PDPD.

Personal Data Protection Measures in Practice

Risk-based approach

Personal data protection is not only an obligation under the laws, it is becoming more and more important given the increasing value of personal data. Businesses are adopting comprehensive data protection protocols to ensure data confidentiality, integrity, and availability. The PDPD frequently uses the term "appropriate measures", particularly in relation to data protection, security, and compliance with obligations. The term refers to actions, safeguards, and controls that organizations must implement to protect personal data in line with PDPD principles.

However, PDPD does not prescribe specific measures, as what is considered "appropriate" depends on the context, risk, and nature of data processing. Risk-based approach is a systematic way of identifying, assessing, and prioritizing risks, meaning that measures should be proportionate to the risk posed to the individuals' rights and freedoms. The appropriateness of measure depends on:

Nature, scope, context, and purpose of processing	• What type of personal data is being processed?; • How much data is being processed?; • Why is the data being processed?
Risk to individuals' rights and freedoms	• Likelihood and severity of risks; • Potential impact if the data is breached or misused.
Cost of control implementation	• Current industry best practices and technology advancements; • Feasibility of implementation, considering resources and costs.
Legal and regulatory requirements:	• Compliance with PDPD and other applicable laws; • Expectations from regulators and industry standards.

Technical and organisational measures (TOMs)

In reality, the personal data protection measures can be broadly divided into 02 types:

Organizational measures	• Assign competent individuals and departments in charge of personal data protection with clear powers and duties; • Draft data protection policies: Data protection framework, Access control policy, Breach response procedure, Personnel training policy, Asset management policy, Data retention policy, Third party management policy, etc.; • Govern data processing and data sharing with third parties via standard agreements or procedures; • Conduct regular training sessions for all employees to ensure they understand their roles and responsibilities in protecting personal data; • Develop procedures for responding to data subject requests, such as requests for access, rectification, erasure, restriction, portability, and objection; • Keep detailed records of all data processing activities; • Designate a DPO. The DPO is responsible for monitoring compliance with the law and regulation, advising the organization on data protection matters, and acting as a point of contact for data subjects and supervisory authorities; • Integrate privacy considerations into product development, IT systems, and business processes from the early stage; • Conduct DPIAs before processing personal data, such as health, financial, or large-scale data processing, etc.
Technical measures	***Measures applied to the data such as:*** • Use encryption techniques to protect personal data both in transit and at rest; • Apply pseudonymization techniques to replace personal data with pseudonyms; • Data partitioning to increase processing efficiency and reduce the damages in case of breach; etc. ***Measures applied to processing systems such as:*** • Implement secure authentication mechanisms, such as strong passwords, multi-factor authentication, and biometric verification; • Implement Security Information and Event Management (SIEM) systems to monitor and detect suspicious activities in real time; • Enable anomaly detection and behavioral analytics to identify unauthorized access attempts; • Establish a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of data processing; • Collect and process only the minimum amount of personal data necessary for the intended purpose; • Back up data regularly in case of accidental or deliberate unauthorized erasure; • Develop and follow secure data disposal procedures to ensure that personal data is permanently deleted or anonymized when it is no longer needed; • Update all applications regularly; • Set up physical controls to restrict access to data storage sites; • Set up environmental controls (against fire, flood, interrupted power supply, etc.) to ensure the continuous operation of the systems; etc.

Privacy by Design and by Default

Article 26 of the PDPD states that personal data protection measures must be implemented from the beginning and throughout the processing of personal data. In order to accomplish this, it is best that the principles of Privacy by Design (PbDs) and Privacy by Default (PbDf) be observed. These principles are even prescribed as an obligation in the GDPR itself.[132]

PbDs can be understood as protecting data through design choices. Instead of treating personal data protection as an afterthought, PbDs require that this element be treated as an essential aspect and integrated into the design of the personal data processing technology and process from the beginning. The objective of PbDs is to prevent privacy issues by addressing them from the root. By observing this principle, organizations can comply with privacy regulations, reduce the risks of privacy breaches, increase consumers' trust and create a culture of privacy. However, PbDs can also be quite challenging since it would require significant upfront investment which smaller organizations may not have, and balancing usability with privacy features can be quite difficult. Examples of PbDs can include actions such as designing an app that encrypts data and limits data sharing from the development stage, or including a Do Not Track feature in web browsers.

PbDf, on the other hand, focuses on configuring systems and services to provide the highest level of privacy settings by default and requires little to no action from the user to ensure their privacy is protected. In other words, the default state of the system must be the one with the highest level of personal data protection. This is to protect user data without requiring any adjustment and interference from the user. The main focus of PbDf is minimizing data collection, sharing, and processing, usually through default settings and configurations. This simplifies privacy for users and reduces the likelihood of user mistakes. However, PbDf may limit the functionality or customization options of the users. Examples of PbDf can include a social media platform making all user profiles private by default, or a platform automatically opting users out of marketing emails and setting visibility of user history to private.

In this day and age where personal data and privacy are more important than ever, PbDs and PbDf are no longer options that organizations can choose to implement or not, instead, they have become necessities. Without them, businesses can face serious risks such as personal data violations, losing consumers' trust, legal and financial troubles, disruptions to operations, and falling behind competitors, etc.

Implementing PbDs and PbDf would require a comprehensive plan and process from choosing the appropriate standards, assessing the current situation and gaps, and formulating measures to be applied and how to apply them, to actual implementation, monitoring, and updating. Taking into account the complexity and scale of data processing, it would be best for organizations to integrate these principles into their operations as soon as possible to save costs and gain an edge over competitors.

Personal Data Protection Certifications

For Organizations

Among current certifications on personal data protection, the ISO 27001 and ISO 27701 are some of the most widely recognized. The International Organization for Standardization (ISO) is an independent, non-governmental international organization that develops and publishes standards across various industries to ensure quality, safety, efficiency, and interoperability. Founded in 1947 and headquartered in Geneva, Switzerland, ISO brings together national standards bodies from over 160 countries to create globally recognized benchmarks that support international trade and innovation. ISO standards cover a wide range of topics, from technology and manufacturing to environmental and data security management. By establishing clear guidelines and best practices, ISO helps organizations improve their processes, meet regulatory requirements, and increase customer trust.

ISO 27001 specifies the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). The primary focus is on managing and securing sensitive company and customer information, minimizing risks associated with data breaches, and protecting data confidentiality, integrity, and availability. ISO 27001 follows a risk-based approach to information security, outlining specific controls across various domains, including access control, cryptography, physical security, incident response, and compliance. Organizations can be certified for ISO 27001 through independent certification bodies, demonstrating a commitment to information security best practices.

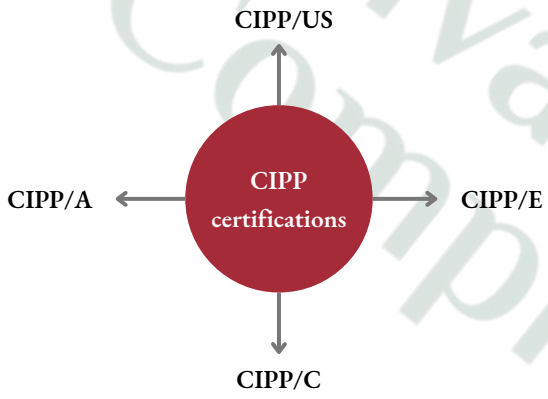
ISO 27701 extends ISO 27001 by adding requirements for a Privacy Information Management System (PIMS) to help organizations manage personal data and ensure compliance with data protection regulations (e.g., GDPR, CCPA). The focus of ISO 27701 is on managing privacy risks associated with Personally Identifiable Information (PII) and improving transparency, accountability, and security related to personal data processing. ISO 27701 includes guidance on PII controllers and processors, specifying roles, responsibilities, and privacy-specific controls that complement the security controls in ISO 27001. ISO 27701 is not an independent standard; it acts as an extension to ISO 27001. Organizations already certified in ISO 27001 can seek additional certification under ISO 27701 to demonstrate their commitment to privacy.

ISO 27001 is foundational for organizations looking to manage information security risks, while ISO 27701 is an important extension for those who also need to ensure compliance with privacy laws. Together, they form a comprehensive approach to securing information and protecting personal data in an increasingly regulated environment.

For Individuals

There are currently many independent organizations offering personal data training and certifications for individuals, among them, the International Association of Privacy Professionals ("IAPP") stands out as the most prestigious. The IAPP offers a set of certifications that would attest to one's capabilities as a privacy professional. Such certifications include:

- **Certified Information Privacy Professional (CIPP)**. The **CIPP** certification is aimed at professionals who need an in-depth understanding of privacy laws, regulations, and frameworks. It's globally recognized and has regional specializations. There are many different CIPP certifications corresponding to different legal jurisdictions in the world such as:



- **CIPP/E:** Focuses on European regulations, including GDPR and ePrivacy Directive.
- **CIPP/US:** Focuses on U.S. laws, including HIPAA, COPPA, FCRA, and CCPA.
- **CIPP/C:** Focuses on Canadian privacy laws such as PIPEDA.
- **CIPP/A:** Focuses on Asian privacy laws in jurisdictions like Singapore, Hong Kong, and India

These certifications would be suitable for privacy officers, data protection officers (DPOs), compliance officers, legal advisors, and anyone involved in privacy program management.

- **Certified Information Privacy Manager (CIPM)**. The **CIPM** certification focuses on implementing and managing privacy programs within organizations. It covers the operational aspects of data protection and privacy, such as governance, risk assessments, privacy metrics, and data life cycle management, IT Privacy program governance and framework development. This certification is suitable for privacy managers, program managers, compliance officers, and others who oversee privacy operations and compliance in organizations.

- **Certified Information Privacy Technologist (CIPT)**. The **CIPT** certification is designed for IT and security professionals who need to understand how to implement privacy by design in technology systems and software. It covers topics such as privacy considerations in technology systems, product design, and software development, strategies for implementing privacy in data architecture and system administration, and understanding emerging technologies like AI and their privacy implications. IT professionals, security engineers, software developers, and systems administrators focused on embedding privacy into technology solutions should consider getting this certification.

Closing Remark

The Vietnam Data Protection Handbook serves as an indispensable guide to navigating the intricate maze of data protection laws and regulations in Vietnam. As demonstrated throughout this Handbook, Vietnam's privacy and data protection legal landscape is evolving rapidly to keep pace with technological advancements and global standards. With the enactment of the PDPD and other relevant regulations, as well as the drafting of a Personal Data Protection Law, Vietnam has taken significant strides towards establishing a robust framework for the protection of data.

Understanding these developments is crucial for organizations operating in Vietnam, as compliance with personal data laws is not just a legal requirement but also a vital component of building consumer trust and safeguarding reputational integrity. As such, the Handbook provides a comprehensive view of the current and possible future legal framework for data protection in Vietnam, from the overarching principles and data subject rights to the responsibilities of data controllers, and processors, as well as the current and possible sanctions for non-compliance.

Additionally, the Handbook also goes into sector-specific regulations on data protection to underscore the need for tailored approaches to data protection across industries such as banking, labor, information technology, and cyberspace. Organizations must implement robust data protection measures, such as Privacy by Design and by Default, to ensure data security from the outset. Certifications and audits further reinforce accountability, fostering a culture of responsible data processing.

As the regulatory environment continues to evolve, businesses and individuals must remain proactive in adapting to new requirements and best practices. The Handbook demonstrates that compliance is not a one-time effort but an ongoing commitment to data ethics, transparency, and security. By embracing a strong personal data protection framework, organizations can mitigate risks, enhance consumer confidence, and contribute to a safer digital ecosystem.

In closing, the Vietnam Data Protection Handbook serves as a comprehensive resource for organizations, legal professionals, and policymakers seeking to navigate Vietnam's data protection landscape with confidence. By providing insights into the legal framework, and practical guidance on compliance, this Handbook empowers stakeholders to uphold privacy rights and foster a culture of trust in the digital age. As Vietnam continues to embrace digital transformation, adherence to privacy and data protection laws will be paramount in safeguarding individuals' rights and promoting responsible data stewardship.

Privacy Compliance

PRIVACYCOMPLIANCE

INTRODUCTION

Pioneering privacy solutions in Vietnam

About PrivacyCompliance

At **PrivacyCompliance**, we see a strong connection between ethical business practices and societal well-being. Our mission is to lead the way in privacy compliance in Vietnam, helping businesses navigate the evolving landscape of data protection. In today's world, consumers, employees, and investors gravitate toward companies that prioritize both people and the planet. As expectations shift—driven by younger generations and rapid technological advancements—businesses must adapt to remain relevant and responsible. We believe that, with the right approach, any organization can thrive in this new era.

What makes **PrivacyCompliance** stand out is our seamless fusion of technology and legal expertise. We craft smart, cost-effective solutions that keep data moving securely while ensuring full compliance with both local and global regulations. Our team is composed of top-tier professionals with deep experience in cybersecurity, legal compliance, data protection, and risk management. We bring an international perspective to every challenge. With industry-leading certifications—including CIPP/E, CIPM, CISM, CISA, CRISC, ISMS LA, and more—we have the knowledge and confidence to address complex privacy issues and provide the highest level of service.

Contact

PrivacyCompliance
Email: info@privacycompliance.vn
Tel: +84 964 899 109
Website: privacycompliance.vn
Add: 5th floor, Diamond Flower Tower, Hoang Dao Thuy street, Thanh Xuan district, Hanoi, Vietnam

Our services

Compliance

We offer a comprehensive range of services to ensure your organization's compliance with applicable laws in a timely and effective manner.

Risk Management

We provide evaluation and mitigation of data security threats, as well as assist you and your organization in earning reputable credentials.

Technology

Our suite of technological products provides comprehensive support for your organization's fundamental security and data privacy requirements.

Compliance solutions

Privacy Review and Assessment

Conduct a review of the basis for the data processing to ensure the compliance of your data system with legal requirements

Policy Management

Upgrade and complement your privacy document arrangement with our drafting and review of Data Privacy Framework, Privacy Policy, Privacy Notice, Technical and Organizational Measures Application (TOMs)

Privacy Impact Assessments (PIAs)

Personal data protection impact assessment (DPIA) and oversea data transfer impact assessment (DTIA) are legal obligations that your organization must comply with, and we can help to facilitate your completion of such assessments

DPO Outsourcing Service

Our outsourced Data Protection Officer (DPO) helps you with managing personal data flow – a highly specialized task that requires a specialist with data protection expertise

Training and Awareness

Build your privacy-prioritized team with a profound understanding of data protection via courses designed by privacy & data governance experts

Risk management solutions

Enterprise Risk Management

Assess and manage the existing and potential risks to the confidentiality, integrity, and availability of your information assets to help you achieve an acceptable risk level among operations

Second-Party Audit

Second-party audit helps to assess and mitigate the information security risks posed by your suppliers and their compliance level – a confirmation of their suitability and compliance with your requirements set out in the contracts

Certification consultation

Provide you with the preparation, establishment, and continual improvement of your privacy information management system to meet the demands of the ISO standards for managing information security risks, which can generally boost your internal energy as well as external reputation

Certification training

The training courses on The Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), and Certified in Cybersecurity (CC) would help you to prepare for the exams for these three credentials which are some of the most respected in the cybersecurity industry

Technology solutions

Data Privacy Management Platform

Our product suite assists your organization in all foundational aspects of security and privacy compliance. We systematically investigate your security posture and provide in-depth recommendations for improvement

Intelligent Data Discovery

Our Intelligent Data Discovery Framework allows your organization to assess and prioritize assets for protection, particularly data such as credit cards, bank account info, with close to zero false positives

Privacy-preserving Technologies

We help your organization with privacy-preserving data processing technologies and offer expertise in advanced cryptographic techniques to protect and preserve the security and privacy of your data

Privacy Compliance Virtual Assistant

Our advanced AI-based virtual assistant provides you with consultancy regarding the security and privacy aspects of your organization. It enables your organization to quickly comply with security & privacy standards and regulations

References

[1] GDPR, Art 83.

[2] Personal Information Protection Law (Peoples' Republic of China) ("PIPL"), Art 66.

[3] 1946 Constitution (Democratic Republic of Vietnam), Art 11.

[4] Bach Thi Nha Nam, Nguyen Ngoc Phuong Hong "Addressing the Challenges of Data Privacy Protection Law in Vietnam", VNU Journal of Science: Legal Studies, Vol. 39, No. 1 (2023) 30-44.

[5] 2013 Constitution (Socialist Republic of Vietnam), Art 21.

[6] 1995 Civil Code (Socialist Republic of Vietnam), Art 34.

[7] The Ministry of Public Security is responsible for exercising state management in safeguarding national security, ensuring social order and safety, combating and preventing crimes and violations of laws concerning national security, social order, and safety, and building the People's Public Security force.

[8] Ministry of Public Security, 'Report assessing the impacts of the policies in the proposal for the drafting of Personal Data Protection Law' (01 March 2024).

[9] Decree 13/2023/ND-CP (Socialist Republic of Vietnam) ("PDPD"), Art 1(1).

[10] PDPD, Art 1(2).

[11] PDPD, Art 2(1).

[12] PDPD, Art 2(4).

[13] PDPD, Art 2(3).

[14] PDPD, Art 2(7).

[15] PDPD, Art 2(6).

[16] PDPD, Art 2(9).

[17] PDPD, Art 2(10).

[18] PDPD, Art 2(11).

[19] PDPD, Art 2(12).

[20] PDPD, Art 2(14).

[21] PDPD, Art 2(8).

[22] PDPD, Art 9.

[23] PDPD, Art 10.

[24] PDPD, Art 24(3).

[25] PDPD, Art 24(4).

[26] PDPD, Art 25(3).

[27] PDPD, Art 24(6) and 25(6).

[28] https://baovedlcn.gov.vn/

[29] PDPD, Art 24(4).

[30] PDPD, Art 25(3).

[31] PDPD, Art 25(6).

[32] PDPD, Art 25(4).

[33] PDPD, Art 28(2).

[34] PDPD, Art 23(1).

[35] PDPD, Art 23(2).

[36] PDPD, Art 23(3).

[37] PDPD, Art 23(4).

[38] PDPD, Art 23(5).

[39] PDPD, Art 23(6).

[40] PDPD, Art 9(2).

[41] PDPD, Art 11(1).

[42] PDPD art 11(2).

[43] PDPD, Art 11(3).

[44] PDPD, Art 11(5).

[45] PDPD, Art 11(6).

[46] PDPD, Art 11(4).

[47] PDPD, Art 11(7).

[48] PDPD, Art 17.

[49] PDPD, Art 18.

[50] PDPD, Art 13(1).

[51] PDPD, Art 13(4).

[52] PDPD, Art 13(2).

[53] PDPD, Art 13(3).

[54] PDPD, Art 19(1).

[55] PDPD, Art 21(1).

[56] PDPD, Art 21(2).

[57] Law on Children No. 102/2016/QH13 (Socialist Republic of Vietnam), Art 1.

[58] The opinion of a child aged seven or older regarding who will directly raise them after a divorce will be taken into consideration, in accordance with Article 81(2) of the Law on Marriage and Family No.52/2014/QH13, dated June 26, 2014.

[59] European Commission, "Information for Individuals" <https://commission.europa.eu/law/law-topic/data-protection/information-individuals_en#consent-in-data-protection>.

[60] PDPD, Art 15.

[61] PDPD, Art 12.

[62] PDPD, Art 16.

[63] Delisting allows individuals to request search engines to remove links to information about them if it is outdated, irrelevant, or excessive, balancing individual privacy against public interest.

[64] PDPD, Art 14.

[65] PDPD, Art 9(6).

[66] PDPD, Art 9(8).

[67] PDPD, Art 9(9).

[68] PDPD, Art 9(10).

[69] PDPD, Art 9(11).

[70] GDPR, Art 12(3).

[71] PDPD, Art 43(2) and 43(3).

[72] PDPD, Art 38(4).

[73] PDPD, Art 39(2).

[74] PDPD, Art 39(5).

[75] PDPD, Art 29.

[76] The fine amounts apply to the administrative violations of an organization.

[77] PDPD, Art 25(8).

[78] Draft Law, Art 2(1).

[79] Draft Law, Art 2(4).

[80] ibid.

[81] Draft Law, Art 2(18).

[82] Draft Law, Art 2(20).

[83] Draft Law, Art 4(2).

[84] Draft Law, Art 8(6).

[85] Draft Law, Art 8(8).

[86] Draft Law, Art 13-15.

[87] Draft Law, Art 15(3).

[88] Draft Law, Art 23(4).

[89] Draft Law, Art 23(5)(b).

[90] Draft Law, Art 25(2).

[91] Draft Law, Art 24(3).

[92] Draft Law, Art 24(6) and Art 25(3).

[93] Draft Law, Art 28(2).

[94] **Article 16. Obligations to provide information before conclusion of an employment contract**
...
2. The employee shall provide the employer with truthful information about his/her full name, date of birth, gender, residence, educational level, occupational skills and qualifications, health conditions and other issues directly related to the conclusion of the employment contract which are requested by the employer.

[95] Draft Law, Art 30.

[96] Draft Law, Art 34(1).

[97] Draft Law, Art 34(2).

[98] Draft Law, Art 34(4).

[99] Draft Law, Art 41(1).

[100] Draft Law, Art 40.

[101] Draft Law, Art 43.

[102] Draft Law, Art 44(2).

[103] Draft Law, Art 47.

[104] Draft Law, Art 45(8) and Art 46(10).

[105] Draft Law, Art 49(3).

[106] Draft Law, Art 49(5).

[107] Draft Law, Art 68(3).

[108] Draft Law, Art 68(1) and Art 68(2).

[109] Draft Law, Art 57.

[110] Exception: there are some obligations that shall be mandated after January 01, 2025.

[111] Law on Consumers' Rights Protection 2023 (Socialist Republic of Vietnam) ("Law on Consumers' Rights Protection 2023"), Art 15.

[112] Law on Consumers' Rights Protection 2023, Art 3(3).

[113] Law on Consumers' Rights Protection 2023, Art 16.

[114] Law on Consumers' Rights Protection 2023, Art 17(1).

[115] Law on Consumers' Rights Protection 2023, Art 17(2).

[116] Law on Consumers' Rights Protection 2023, Art 18(3).

[117] Law on Consumers' Rights Protection 2023, Art 18(4).

[118] Law on Consumers' Rights Protection 2023, Art 19(1).

[119] Law on Consumers' Rights Protection 2023, Art 19(2).

[120] Law on Consumers' Rights Protection 2023, Art 20(1) and 20(2).

[121] Law on Consumers' Rights Protection 2023, Art 20(3).

[122] Labor Code 2019 , Art 16(2).

[123] Law on Cyberinformation Security 2015 (Socialist Republic of Vietnam) ("Law on Cyberinformation Security 2015"), Art 17(3).

[124] Law on Cyberinformation Security 2015, Art 18(1).

[125] Law on Cyberinformation Security 2015, Art 18(2).

[126] Law on Cyberinformation Security 2015, Art 18(3).

[127] Law on Cyberinformation Security 2015, Art 19.

[128] **Article 30. Cybersecurity forces**
Cybersecurity forces include:
1. Professional cybersecurity forces of the Ministry of Public Security and the Ministry of National Defense.
2. Cybersecurity forces of other Ministries, agencies, the People's Committees of provinces and organizations managing national security information systems.
3. Other organizations and individuals mobilized to participate in cybersecurity protection.

[129] PDPD, Art 26.

[130] PDPD, Art 27.

[131] PDPD, Art 28.

[132] GDPR, Art 25.

PrivacyCompliance., JSC

Email: info@privacycompliance.vn
Tel: +84 (0) 964 899 109
Website: privacycompliance.vn
Add: 5th Floor, Diamond Flower Tower, Hoang Dao Thuy Street, Nhan Chinh Ward, Thanh Xuan, Hanoi, Vietnam