Guideline

PERSONAL DATA RETENTION

Document Code	**05e-HD/SG/HDCV/FSOFT**
Version	**3.5**
Effective date	**01-Dec-2024**

TABLE OF CONTENT

RECORD OF CHANGE

No	Effective Date	Version	Change Description	Reason	Reviewer ADPO	Final Reviewer GDPO	Approver Board member
1	10-May-2019	1.0	Newly issued	Legal requirement	Minh	Michael Hering	CFO/COO
2	21-Oct-2019	1.1	Add content of section Introduction-Adjust the purpose-Adjust application scope-Add some new definitions-Change related documents-1.5-Responsibilities: Change DPO to GDPO, leading to adjustment of responsibilities.	Legal requirement	Trang	Michael Hering	CFO/COO
3	11-May-2020	2.1	-Add sections:1.3. Application of national Laws, 2.10. Data Protection Records, 2.11. Email Data Records, 2.12. Communication Data Records -Update 1.2. Application Scope and 1.5. Related Documents Update: 2.3. Purchasing/Order, 2.7. Data proceed in behalf a customer and 2.9. Customer Data -Change: “2.8. Employee Data” into “2.8.” Employee Data/ Personnel Records and update 2.8	Update according to annually revision requirement	Trang	Michael Hering	CFO/COO
4	01-Jul-2020	2.1.1	HITRUST	HITRUST requirement	Trang	Michael Hering	CFO/COO
5	19-Oct-2020	2.2	Update sections: related document, Data Protection Records	Legal requirement	Trang	Michael Hering	CFO/COO
6	01-May-2021	3.0	Change the document structure. Update sections: Application Scope and Related Document	Legal requirement	Trang	Michael Hering	CFO/COO
7	01-Oct-2021	3.1	1 added: FPT Software Personal Data Protection Handbook and ISM guidelines, 1.2 added: statement_PIMS scope_V1.0, 1.4 added: procedure_Retention of Records_V1.0, record_retention schedule_V1.0, 2.10 added: until 2021, from 01.10.2021 processed, maintained and stored by DPO Tool (WEB application on MS Azure), record_retention schedule_V1.0, 2.7 added Temporary files 3.2 added: procedure_Retention of Records_V1.0	Legal requirement	Trang	Michael Hering	CFO/COO

No	Effective Date	Version	Change Description	Reason	Reviewer ADPO	Final Reviewer GDPO	Approver Board member
8	01-Apr-2022	3.2	3.2 13 added PIPL, 3.2 14 added: PDPL, UAR, Decree-Law No. 45 of 2021 3.2 16 added: Decree of the Vietnamese Government: Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân 3.2 17 PDP_ Handbook_Version_V3.2 3.2 18: 11e-QT/SG/HDCV/FSOFT		Linh Do Thi Dieu	Michael Hering	CFO/COO
9	01-Nov-2022	3.3	Deleted 2.10 until 30.09.2021, from 01.10.2021 processed, maintained and stored by DPO Tool (WEB application on MS Azure). Added 3.3. Data Protection Law, Vietnam, Overview. Added 3.2 15 Republic Act 10173 Data privacy Act 2012 Added 3.2 17 PDPA Added 3.2 18 TISAX	Biannually revision	Linh Do Thi Dieu	Michael Hering	CFO/COO
10	01-Aug-2023	3.4	Adjust document version numbers added 3.2 14, 18 changed 3.2 22: Came in force 07/2023 changed 3.3 PDPD was finalized and was coming in force 07/2023	Biannually revision	Linh Do Thi Dieu	Michael Hering	CFO/COO
11	14-May-2024	3.4.1	change document classification, from 'internal use' to 'public'	Document classification	Linh Do Thi Dieu	Michael Hering	CFO/COO
12	01-Dec-2024	3.5	Version numbers 1. ,1.1, 2. Added PDPD13, 2.9 replace CRM/CRM2 with salesforce Added 2.9 under Vietnamese law only Added 3 Deletion and Destruction of Personal Data added 4.2.18 Changed 4.2 7 t0 March 15, 2024	ISO27701 requirements	Linh Do Thi Dieu	Michael Hering	CFO/COO

1 INTRODUCTION

FPT Software Company, Ltd. ("FPT Software" hereinafter) Corporate Data Protection Policy, guidelines, procedures, and templates lay out strict requirements for processing personal data pertaining to customers, business partners, employees or any other individual. It meets the requirements of the European Data Protection Regulation/Directive as well as other national Data Protection Regulations and ensures compliance with the principles of national and international data protection laws in force all over the world. The policy, guidelines and templates set a globally applicable data protection and security standard for FPT Software and regulates the sharing of information between FPT Software, subsidiaries, and legal entities. FPT Software have established guiding data protection principles – among them transparency, data economy and data security – as FPT Software Personal Data Protection Handbook and ISM guidelines.

The General Data Protection Regulation (GDPR) defines “personal data” as any information relating to an identified or identifiable natural person (a “data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR also addresses “special category” personal data (also known as “sensitive” personal data). Such data includes, but is not necessarily limited to, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organizational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure (“the right to be forgotten”). Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

- Where the personal data is no longer required for the purpose for which it was originally collected or processed
- If the data subject withdraws their consent
- If the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest
- If the personal data is processed unlawfully
- If the personal data must be erased to comply with a legal obligation

- Where the personal data is processed for the provision of information society services to a child.

1.1 Purpose

This guideline sets out the type(s) of personal data processed by FPT Software for specific purpose(s)), the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with the GDPR, PDPD13 and other personal data protection acts, please refer to FPT Software Personal Data Protection Management Policy.

For those activities that didn't list below, the data should not be stored and require destroying immediately.

1.2 Application Scope

See Policy_PIMS scope_V1.4.

This guideline is binding for all departments and functions globally which are involved in personal identifiable information processing. Every FPT Software department, legal entity or subsidiary must follow this guideline.

1.3 Application of national Laws

The Data Protection Policy, guidelines and templates comprises the internationally accepted data privacy principles without replacing the existing national laws. It supplements the national data privacy laws. The relevant national law will take precedence in the event that it conflicts with the Data Protection Policy and guidelines, or it has stricter requirements than this Policy and guidelines. The content of the Data Protection Policy and guidelines must also be observed in the absence of corresponding national legislation. The reporting requirements for data processing under national laws must be observed.

Each subsidiary or legal entity of FPT Software is responsible for compliance with the Data Protection Policy, this guideline and the legal obligations. If there is reason to believe that legal obligations contradict the duties under the Data Protection Policy or the guidelines, the relevant subsidiary or legal entity must inform the Global Data Protection Officer. In the event of conflicts between national legislation, the Data Protection Policy, and this guideline, FPT Software GDPO will work with the relevant subsidiary or legal entity of FPT Software to find a practical solution that meets the purpose of the Data Protection Policy and this guideline.

1.4 Responsibility

The Global Data Protection Officer, appointed by the FPT Software Board Member responsible for Data Protection on behalf of the CEO of FPT Software is fully responsible.

The Global Data Protection Officer (GDPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). The GDPO is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements and other Personal Data Protection Acts. The primary role of the GDPO is to ensure that organization processes, the personal data of employees, customers, providers, or any other individuals are in compliance with the applicable data protection rules. GDPO should be able to perform the duties independently.

GDPO is responsible for observation of the time limits for personal date retention. GDPO will manage the retention in Template_Retention and Disposal Schedule _v1.4 for all documents or information he is the owner from following Procedure_Retention of Records_V1.4. GDPO will ensure that all departments, units, subsidiaries, and legal entities of the FPT Software are following the FPT Software's guidelines and the respective laws.

2 GUIDELINE CONTENT

2.1 Abbreviations

AC - After Completion

ACT - While Employed or Active AF - After End of Fiscal Year

AT - After Termination

OBS - Obsolete

P - Permanent

SUP - Save Until Superseded

2.2 Member Account Information

Registered account information will be maintained lifetime unless Data Subject exercise his/her right to erasure.

2.3 Purchasing/Order

Online Order	AC+2 years
Payment information	AC+2 years
Billing information	AC+2 years

2.4 Service Operation

Order for Repair	2 years
RMA	2 years

*(A **return merchandise authorization** (**RMA**) is a part of the process of returning a product to receive a refund, replacement, or repair during the product's warranty period*).

2.5 Report Generation/Transfer

All reports generated shall not contain any Data Subject identifiable data. The report generator shall view the content and remove the Data Subject's identifiable data unless such Data Subject's identifiable data is necessary for business report and reviewed and approved by Privacy GDPO. The review record shall be kept for 3 years.

2.6 Test Data

Data used for application testing must be masked, anonymized or pseudonymized where every it is possible (see Guideline_Pseudonymisation Minimisation and Encryption_v1.5). If it is not possible the personal data must be deleted immediately after application testing is finished.

2.7 Temporary Files

FPT Software IT department must ensure that temporary files created by FPT Software IT system are deleted if they are not needed for information processing anymore.

IT systems are creating temporary files in the normal course of their operation. Such files are specific to the system or application but may include file system roll-back journals and temporary files associated with the updating of databases and the operation of other application software. Temporary files are not needed after the related information processing task has completed but there are circumstances in which they cannot be deleted. The length of time for which these files remain in use is not always deterministic but a “temporary file check” procedure should identify the relevant files and determine how long it has been since they were last used. IT and ISM departments are responsibly to implement a “temporary file check” procedure. This procedure must be executed quarterly, and temporary files must be deleted if they are 3 month not used.

2.8 Data proceed in behalf a customer

In case FPT Software (data processor) is processing on behalf of a customer (data controller), FPT Software must follow exactly the instructions of the data controller. If the contract with the customer is terminated, all personal data must be erased immediately.

2.9 Employee Data/Personnel Records

Record type/Category	**Retention period**
Commissions, Bonuses, Incentives, Awards	7 years, or based on applicable national laws/regulations
Employer Information Reports	2 years after superseded or filing (whichever is longer), or based on applicable national laws/regulations
Employee Earnings Records, payroll information, Payroll records – salaries and other payments through payroll	Separation + 6 years, or based on applicable national laws/regulations
Payroll records - Maternity, Paternity, Adoption and SSP records	3 years after end of AF

Record type/Category	Retention period
Pension, social insurance details - name, National Insurance number, opt-in notice and joining notice	6 years after effective date
Employee Handbooks	1 copy kept permanently
Employee Medical Records	Separation + 6 years, or based on applicable national laws/regulations
Employee Medical Records	Separation + 6 years, or based on applicable national laws/regulations
Employee Personnel Records (including individual attendance records, application forms, job or status change records, performance evaluations, termination papers, withholding information, garnishments, test results, training, and qualification records)	Separation + 6 years, or based on applicable national laws/regulations
Timesheet information, Timecards/Sheets	24 months, or based on applicable national laws/regulations
Candidate records, hiring process, CV (rejected candidates)	12 months, or based on applicable national laws/regulations
Job applications and interview records for unsuccessful applicants	6 months, after interview or based on applicable national laws/regulations
Employment Contracts – Individual	Separation + 7 years, or based on applicable national laws/regulations
Employment Records - Correspondence with Employment Agencies and Advertisements for Job Openings	3 years from date of hiring decision, or based on applicable national laws/regulations
Employment Records - All Non-Hired Applicants (including all applications and resumes - whether solicited or	2 years, or based on applicable national laws/regulations

Record type/Category	Retention period
unsolicited, results of post-offer, pre-employment physicals, results of background investigations, if any, related correspondence)	
Job Descriptions	3 years after superseded
All other HR documents	1 year after end of employment

Under Vietnamese law only: (Legal basis updated 10/2022/TT-BNV)

Record type/Category	Retention period
Organization and employee records: org chart, appointment, promotion, transfer, rotation of staff, Statistical report on list, quantity and quality of staff, merger, consolidation, separation, dissolution of agencies and affiliated units	20 years
Basic Personal information list: Includes name, address, phone number, date of birth, nationality and other personal information about the employee.	20 years
Recruitment records: Includes information about the employee's recruitment process, such as job application, copies of resumes, qualifications, identification documents, letters of recommendation, and interview results. - Report on results, list of successful candidates - Application documents, exam papers, exam organization documents	70 years

Employment Contracts: Includes contracts, agreements and terms of employment and employee benefits.	70 years
Work history: Includes information about work history, job position, department, date of employment, promotions and advancements.	20 years
Salary and benefits: Includes information on salary, benefits, bonuses, tax deductions and records related to salary payments	20 years
Training and Development: Includes information about training courses, certifications, personal development programs, and employee skills.	10 years
Discipline and feedback: Includes documents related to discipline, warnings, performance reviews, and feedback from management.	20 years
Trade Union records: Records of implementation of major campaigns and resolutions of Trade Union Materials on organizations, personnel and activities of Trade Union	20 years
Insurance claim records: Records of social insurance, health insurance, unemployment insurance, occupational accident and disease insurance	70 years
Rewarding and recognition records (citizens and expats)	5 Years
Original records of employee	70 years
Employee profile record management	70 years

2.10 Customer Data

Personal Data of customers FPT Software got to support special processes of the customer (for example: VISA application) must be erased immediately after the process is finalized.

Data about customer Saleforce, SanSan, customer care application retention period 2 years or based on applicable national laws/regulations.

2.10 Data Protection Records

Record type/Category	Retention period
Data Subject Consent	6 years after consent expired
Privacy notices, statement, and index	6 years after end of life
Record of Processing Activities	6 years after end of life, stored in data inventory register
Data Subject Rights Request	6 years, stored in incident, complaint, and request register until 30.09.2021.
Data Protection appeals and complaints	6 years, stored in incident, complaint, and request register until 30.09.2021.
Data Protection Incident record	6 years, stored in incident, complaint, and request register.
DP Audit records	6 years, stored in internal audit register
DPIA records	6 years, stored in DPIA register
Data inventory records	6 years after end of service, stored in data inventory register until 30.06.2021.
DP Policies, guideline, templates	6 years after replacement (revision), stored in QMS2. Retention managed in Template_Retention and Disposal Schedule _v1.4

2.11 Email Data Records

Emails can be considered to be business letters: Whenever transactions are prepared, concluded, carried out or canceled via email, the electronic message is then considered a business letter and cannot simply be deleted. Emails are therefore also subject to retention periods. As a rule, emails must be kept in the corporate context for 6 years. However, the rule only applies to business emails. If employees write personal emails to one another, these do not need to be archived.

Mailbox items automatically disposed of 2 years after they were created, sent, or received. All sent and received mailbox items also logged and archived separately for 6 years or based on applicable national laws/regulations.

2.12 Communication Data Records

Communications data is information about an electronic communication—a footprint left after accessing the Internet, sending an email, or making a phone call. It might, for example, include customer registration details, the date, time and duration of a communication, the phone number or email address of the sender and recipient, the amount of data up/downloaded, or the location of a mobile device from which a communication was made.

It is important to recognize, however, that it does not include the actual content of a communication. It is in this way that communications data differs from 'stored communications' (for example, emails and text messages that have already been sent) and telecommunications interception (listening to or recording telephone conversations), both of which are also dealt with very differently.

"Telecommunications data" is information about the process of a communication, as distinct from its content. It includes information about the identity of the sending and receiving parties and related subscriber details, account identifying information collected by the FPT Software or FPT Telecom to establish the account, and information such as the time and date of the communication, its duration, location, and type of communication.

Communications data being data which indicates the 'identity, source, path and destination' of a particular service, which may come from a variety of sources including:

Use data:

- Itemized telephone call records (numbers called).
- Itemized records of connections to internet services.
- Itemized timing and duration of service usage (calls and/or connections).
- Information about amounts of data downloaded and/or uploaded.
- Information about the use made of services which FPT Software employees is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.
- Information about the use of forwarding/redirection services.
- Information about selection of preferential numbers or discount calls.

Traffic data:

- Information tracing the origin or destination of a communication that is in transmission.
- Information identifying the location of equipment when a communication is or has been made or received (such as the location of a mobile phone).
- Information identifying the sender and recipient (including copy recipients) of a communication from data comprised in or attached to the communication.

- Routing information identifying equipment through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed).
- Online tracking of communications.

Retention period 2 years or based on applicable national laws/regulations.

3 DELETION AND DESTRUCTION OF PERSONAL DATA

The deletion and destruction of personal data are carried out in the following cases:

Immediately after the end of the personal data Retention Schedule specified in this guideline,

or

within 3 working days after a request from the data subject, unless otherwise provided by law

(see Procedure_Data Subject Access Request_v1.4, Guideline_Data Subject Right Request_v1.0).

The deletion and destruction of personal data are carried out as follows:

General Principle

Immediately after the end of each retention period, personal data will be securely destroyed, irretrievably deleted, or anonymized in such a way that the data itself or when combined with other data cannot identify any specific individuals (hereinafter referred to as "Destruction of personal data").

Only authorized departments and personnel of the FPT Software are allowed to Destroy personal data. In cases where the Destruction of personal data is delegated to a Personal Data Processor, the delegation must be documented in writing and legally signed by authorized representatives of the parties.

Physical documents containing personal data

The Destruction of physical personal data is carried out by cutting, shredding, pulverizing, recycling, or burning according to the following requirements:

Physical documents containing personal data are destroyed according to the regulations of this guideline and Retention Schedule in this guideline

- It is strictly forbidden to dispose paper documents containing personal data before destruction
- Paper shredders are equipped in necessary areas and are only used to destroy physical personal data, ensuring that the destroyed documents cannot be restored;
- FPT Software applies other necessary and feasible measures to ensure that paper documents cannot be restored or copied;
- The monthly destruction management log must be approved by the competent manager and stored for an appropriate period.

Personal data saved in online tool, system or electronic files containing personal data

The destruction of an electronic file is carried out by irretrievably deleting data using specialized programs (file erasers, file shredders, file pulverizers) or formatting the storage media (e.g., USB), according to the following requirements:

- Electronic files containing personal data are destroyed according to the regulations of this guideline and Retention Schedule in this quideline. The Destruction of personal data includes the destruction of all backups.
- FPT Software may choose to destroy storage media (e.g., USB, mobile SSD) by pulverizing or burning without affecting regulations on special waste management and environmental protection.
- FPT Software applies necessary and feasible measures to ensure that electronic documents cannot be restored or copied. The monthly destruction management log must be approved by the competent manager and stored for an appropriate period.

Management of the deletion and destruction of personal data

The Destruction of personal data must be notified to GDPO,

which will sign a document acknowledging the destruction of personal data with the following

contents:

- The date of the Destruction of personal data;
- Description of the data destroyed/deleted and the method of Destruction of personal data;
- The name of the Employee, personnel responsible for the Destruction of personal data; and
- The process of the Destruction of personal data (when delegated to a Personal Data
- Processor).

GDPO is responsible for notifying, assigning personnel to carry out, and supervising and auditing the process of the Destruction of personal data. The person responsible for managing personal data is in charge of, confirming, and controlling the destruction of personal data activities, ensuring compliance with the regulations of this guideline.

4 APPENDIX

4.1 Definition

Abbreviations	Description
PII, Personal Identifiable Information, Personal Data	Refer to the personal data defined by the EU GDPR (Article 4 (1)), 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Subject	EU GDPR (Article 4 - 1), Data subject refers to any individual person who can be identified, directly or indirectly.
Data Controller	EU GDPR (Article 4 - 7), Data Controller means the natural or legal person, public authority, agency or anybody which alone or jointly with others, determines the purpose and means of processing of personal data; where the purpose and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Data Processor	EU GDPR (Article 4 - 8), Data Processor means a natural or legal person, public authority, agency or anybody which processes data on behalf of the controller.
Recipient	EU GDPR (Article 4 - 9), A natural or legal person, public authority, agency or anybody, to which the personal data are disclosed, whether third party or not.
Third Party	EU GDPR (Article 4 - 10), A natural or legal person, public authority, agency or anybody other than the data subject, controller, processor and persons who under direct authority of controller or processor, are authorized to process personal data
DPO/GDPO/ADPO	Data Protection Officer/Global Data Protection Officer//Assistant Data Protection Officer
DPIA	Data Protection Impacted Assessment
PIMS	Personal Information Management System

Abbreviations	Description
EU	European Union

4.2 Related Documents

No	Code	Name of documents
1	EU GDPR	EU General Data Protection Regulation
2	95/46/EC	EU Data Protection Directive 95/46/EC
3	Privacy shield	EU-U.S. and Swiss-U.S. Privacy Shield Frameworks designed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.
4	APPI	Act on the Protection of Personal Information, Japan. It came into force on 30 May 2017.
5	PDPA	Personal Data Protection Act 2012, Singapore
6	PDPO	Personal Data (Privacy) Ordinance, Hongkong, 2012
7	PIPA	South Korea's substantial Personal Information Protection Act (PIPA) was enacted on March 15, 2024
8	PIPEDA	Personal Information Protection and Electronic Documents Act, Canada 2018
9	Privacy Act, APPs, CDR	Privacy act Australia including Australian Privacy Principles, Consumer Data Right
10	HITRUST	Health Information Trust Alliance (CSF, Common Security Framework)
11	HIPAA	Health Insurance Portability and Accountability Act of 1996 (HIPAA), US
12	PCI DSS	Payment Card Industry Data Security Standard, May 2018
13	CCPA	California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq.
14	VCDPA	Virginia Consumer Data Protection Act, 01/2023
15	PDPL, UAE	Decree-Law No. 45 of 2021

No	Code	Name of documents
16	DPA Philippines	Republic Act 10173, Data privacy Act 2012
17	PIPL	Personal Information Protection Law of the People's Republic of China and related laws and regulations
18	PDPL Indonesia	Data protection in Indonesia is regulated by Law No. 27 of 2022 on Personal Data Protection ("PDP Law")
19	PDPA Thailand	Thailand's Personal Data Protection Act, 06/2022
20	PDPA Malaysia	Personal Data Protection Act 2010, Malaysia
21	TISAX	Trusted information security assessment exchange
22	BS10012: 2017	British Standard Personal Information Management System
23	PDPD13, VN	Decree of the Vietnamese Government: PDPD13 Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân 07/2023
24	FPT Software Personal Data Protection Handbook	PDP_ Handbook_Version_V3.5

4.3 Data Protection Law, Vietnam, Overview

There is no single data protection law in Vietnam. Regulations on data protection and privacy can be found in various legal instruments. The right of privacy and right of reputation, dignity and honour and fundamental principles of such rights are currently provided for in Constitution 2013 ("**Constitution**") and Civil Code 2015 ("**Civil Code**") as inviolable and protected by law.

Regarding personal data, the guiding principles on collection, storage, use, process, disclosure or transfer of personal information are specified in the following main laws and documents:

- **Criminal Code** No. 100/2015/QH13, passed by the National Assembly on 27 November 2015
- Law No. 24/2018/QH14 on Cybersecurity, passed by the National Assembly on 12 June 2018 ("**Cybersecurity Law**");
- Law No. 86/2015/QH13 on Network Information Security, passed by the National Assembly on 19 November 2015; as amended by Law No. 35/2018/QH14 dated 20 November 2018, on amendments to some articles concerning planning of 37 Laws ("**Network Information Security Law**");
- Law No. 59/2010/QH12 on Protection of Consumers' Rights, passed by the National Assembly on 17 November 2010; as amended by Law No.35/2018/QH14 dated 20 November 2018, on amendments to some articles concerning planning of 37 Laws ("**CRPL**");
- Law No. 67/2006/QH11 on Information Technology, passed by the National Assembly on 29 June 2006; as amended by Law No. 21/2017/QH14 dated 14 November 2017 on planning ("**IT Law**");
- Law No. 51/2005/QH11 on E-transactions, passed by the National Assembly on 29 November 2005 ("**E-transactions Law**");
- Decree No. 85/2016/ND-CP dated 1 July 2016, on the security of information systems by classification ("**Decree 85**");
- Decree No. 72/2013/ND-CP dated 15 July 2013 of the Government, on management, provision and use of Internet services and online information; as amended by Decree No. 27/2018/ND-CP dated 1 March 2018 and Decree No.150/2018/ND-CP dated 7 November 2018 ("**Decree 72**");
- Decree No. 52/2013/ND-CP dated 16 May 2013 of the Government; as amended by Decree No. 08/2018/ND-CP dated 15 January 2018, on amendments to certain Decrees related to business conditions under state management of the Ministry of Industry and Trade and Decree No. 85/2021/ND-CP dated 25 September 2021 ("**Decree 52**");
- Decree No. 15/2020/ND-CP of the Government dated 3 February 2020 on penalties for administrative violations against regulations on postal services, telecommunications, radio frequencies, information technology and electronic transactions ("**Decree 15**");

- Circular No. 03/2017/TT-BTTTT of the Ministry of Information and Communications dated 24 April 2017 on guidelines for Decree 85 ("**Circular 03**");
- Circular No. 20/2017/TT-BTTTT dated 12 September 2017 of the Ministry of Information and Communications, providing for Regulations on coordinating and responding to information security incidents nationwide ("**Circular 20**");
- Circular No. 38/2016/TT-BTTTT dated 26 December 2016 of the Ministry of Information and Communications, detailing cross-border provision of public information ("**Circular 38**");
- Circular No. 24/2015/TT-BTTTT dated 18 August 2015 of the Ministry of Information and Communications, providing for the management and use of Internet resources, as amended by Circular No. 06/2019/TT-BTTTT dated 19 July 2019 ("**Circular 25**"); and
- Decision No. 05/2017/QD-TTg of the Prime Minister dated 16 March 2017 on emergency response plans to ensure national cyber-information security ("**Decision 05**").

Applicability of the legal documents will depend on the factual context of each case, e.g businesses in the banking and finance, education, healthcare sectors may be subject to specialized data protection regulations, not to mention to regulations on employees' personal information as provided in Labour Code 2019 ("**Labour Code**").

The most important Vietnamese legal documents regulating data protection are the Cybersecurity Law and Network Information Security Law. Cybersecurity laws in other jurisdictions that were inspired by the GDPR of the EU, the Cybersecurity Law of Vietnam shares similarities with China's Cybersecurity Law enacted in 2017. The law focuses on providing the government with the ability to control the flow of information. The Network Information Security Law enforces data privacy rights for individual data subjects.

A draft Decree detailing a number of articles of the Cybersecurity Law ("**Draft Cybersecurity Decree**"), notably including implementation guidelines for data localization requirements, together with a draft Decree detailing the order of and procedures for application of a number of cybersecurity assurance measures and a draft Decision of the Prime Minister promulgating a List of information systems important for national security, are being prepared by the Ministry of Public Security ("**MPS**") in coordination with other relevant ministries, ministerial-level agencies and bodies.

MPS has drafted a Decree on personal data protection ("**Draft PDPD**"), which is contemplated to consolidate all data protection laws and regulations into one comprehensive data protection law as well as make significant additions and improvements to the existing regulations. The Draft PDPD was released for public comments in February 2021 and was originally scheduled to take effect by December 2021. The Finalization process consuming much more time than the MPS first anticipated. PDPD was finalized and was coming in force 07/2023.