Guideline

PII CLASSIFICATION AND RATING

Document Code	06e-HD/SG/HDCV/FSOFT
Version	3.4
Effective date	01-Aug-2023

TABLE OF CONTENT

RECORD OF CHANGE

No	Effective Date	Version	Change Description	Reason	Reviewer	Final Reviewer	Approver
1	10-May-2019	1.0	Newly issued	Business requirement	MinhPT	Michael Hering	HoanNK
2	21-Oct-2020	1.1	Annually revision	Legal requirement	TrangNN4	Michael Hering	HoanNK
3	11-May-2020	2.0	Add 2 sections: 1.5. Application of national Laws, 2.2. Data Classification Essentials Add content of 1 Introduction Update: 1.1. Purpose, 1.2 Application Scope, 1.3 Definition, 1.4 Related Document, 1.5. Responsibility Update 2. Guideline content Add Example PII at APPENDIX section	Update according to annually revision requirement	TrangNN4	Michael Hering	HoanNK
4	01-Jul-2020	2.0.1	HITRUST	HITRUST requirement	TrangNN4	Michael Hering	HoanNK
5	19-Oct-2020	2.1	Update sections: related document and responsibility	Legal requirement	TrangNN4	Michael Hering	HoanNK
6	01-May-2021	3.0	Change the document restructure. Update sections: Purpose, Responsibility, Data Classification Essentials, Related Document Add 3.3. Example PII	Legal requirement	TrangNN4	Michael Hering	HoanNK
6	01-Oct-2021	3.1	1 added: Personal Data Protection Handbook and IMS guidelines, 1.2 added: statement_PIMS scope_V1.0, 2.2 added: DPO Tool	Legal requirement	TrangNN4	Michael Hering	HoanNK
7	01-Apr-2022	3.2	1.2 added: Policy_PIMS scope_V1.1 3.1 14 added PIPL, 3.1 15 added: PDPL, UAR, Decree-Law No. 45 of 2021 3.1 17 added: Decree of the Vietnamese Government: Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân 3.1 18 PDP_ Handbook_Version_V3.2	Biannually revision	LinhDTD1	Michael Hering	HoanNK

No	Effective Date	Version	Change Description	Reason	Reviewer	Final Reviewer	Approver
8	01-Nov-2022	3.3	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	LinhDTD1	Michael Hering	HoanNK
9	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	LinhDTD1	Michael Hering	HoanNK

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 IMS guidelines.

1.1 Purpose

FPT Software has globally a wide range of personal data collected, used and proceed for FPT Software business process and as well on behalf of our customer as their service. This guideline is a unified version of business conduct involving personal information, collected personal data processing and use of that category and confidentiality level for the benefit of each business unit to take appropriate protective measures to protect personal information.

Personally Identifiable Information (PII) is a legal term pertaining to personal data protection environments. While PII has several formal definitions, generally speaking, it is information that can be used by organizations on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

FPT Software uses the concept of PII to understand which data we store, process, and manage that identifies people and may carry additional responsibility, data protection requirements, and in some cases legal or compliance requirements.

In order to standardize the collection, processing, transfer, and use of personal data, and promote the reasonable, lawfully, fairly and transparent use of personal data to prevent personal data from being stolen, altered, damaged, lost or leaked, FPT Software establishes personal data protection management policy, guidelines and templates.

Data classification tags data according to its type, sensitivity, and value to FPT Software if altered, stolen, or destroyed. It helps to understand the value of data, determine whether the data is at risk, and implement controls to mitigate risks. Data classification also helps to be complied with relevant industry-specific regulatory mandates and data protection laws such as SOX, HIPAA, PCI DSS, ISO 27701, BS 10012:2017, GDPR and other national Personal Data Protection Regulations.

1.2 Application Scope

See Policy_PIMS scope_V1.3.

Also, in scope processes and information systems FPT Software is using on behalf of a customer for the processing and/or transfer of personal data.

1.3 Application of national Laws

This 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 Global Data Protection Officer 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) and other national/international laws/regulation.

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 in compliance with the applicable data protection rules. GDPO should be able to perform the duties independently.

GDPO is responsible to advice, control and execute the development and maintenance of the personal data inventory. GDPO must ensure that all departments of the company are following the company guidelines and the respective laws.

GDPO is responsible for data protection policies, guidelines, and templates.

GDPO is responsible to manage the annually internal audits and reports the audit results to FPT Software board.

Internal Audit Group

Assigned by the GDPO and approved by Board member responsible for DP.
Execution and management the internal audit operations based on GDPO advice.
Development of an internal audit plan approved by the GDPO.
Organize the auditors' education and training.
Report internal audit results to the GDPO.

More details in Guideline_Personal Data Protection Organization_V3.4

2 GUIDELINE CONTENT

2.1 Information Category

FPT Software information must be classified into one of the following categories:

Information Category
Sensitive Personally Identifiable Information (SPII) (GDPR A.9/10, Vietnam law clause PDPD)
Customer Proprietary Network Information (CPNI)
Customer Created Content
Employee Specific Compensation and Benefit Information, Regulatory Review, Assessment, or Audit Information
Protected Health Information (PHI)
Operational Information requiring the highest level of protection
Personally identifiable information (PII)
Employment Information including skill profile
Operational Information requiring a high level of protection
Information on internal FPT Software sites
Operational Information requiring adequate or moderate level of protection
Customers' publicly available information
Information that HR has approved and officially released to public
Information that has been explicitly approved by the appropriate department (e.g. Media Relations, Government Affairs, and Corporate Communications, Investor relations) as suitable for public view and use

2.2 Data Classification Essentials

Successful data classification requires a basic understanding of the following concepts.

Data States:

Data exists in one of three states—at rest, in process, or in transit. Regardless of state, data classified as confidential must remain confidential.

Data Format:

Data can be either structured or unstructured. Structured data are usually human readable and can be indexed. Examples of structured data are database objects and spreadsheets. Unstructured data are usually not human readable or indexable. Examples of unstructured data are source code, documents, and binaries. Classifying structured data is less complex and time-consuming than classifying unstructured data.

Data Discovery:

Classifying data requires knowing the location, volume, and context of data on premises, in the cloud, and in legacy databases (See data inventory: Template_Personal Data Processing Inventory_v2.6 until 30.09.2021, from 01.10.2021 inventory is processed, maintained and stored in DPO Tool, WEB based application on MS Azure, Guideline_Personal Data Inventory Management_v3.4).

Data Sensitivity:

Data is classified according to its sensitivity highly confidential, confidential, internal only and public.

High sensitivity data, if compromised or destroyed in an unauthorized transaction, would have a catastrophic impact on the organization or individual(s). High sensitivity data includes personal data, financial records, legal data, business data such as intellectual property, authentication data, etc.

Medium sensitivity data is for internal use only, but if compromised or destroyed, would not have a catastrophic impact on the organization or individual(s.) Examples of medium sensitivity data are emails and documents that do not include confidential data.

Low sensitivity data is for public use. Examples include press releases, marketing materials, website content.

Compliance Requirements:

Data classification must comply with relevant data protection laws, regulatory and industry-specific mandates, which may require classification of different data attributes. For example, the Cloud Security Alliance (CSA) requires that data and data objects must include data type, jurisdiction of origin and domicile, context, legal constraints, sensitivity, etc. PCI DSS does not require origin or domicile tags.

2.3 Classification Table

If multiple classification categories apply, label and manage information at the highest level of security. For example, the appropriate label for a document containing both Internal and Confidential information is Confidential. Likewise, the appropriate label for a backup tape containing Confidential and Public information then it is Confidential.

Team sites, shared network drives, project sites, collaborative operational SharePoint sites, or similar collaborative operational applications must be classified appropriately based on the highest classification level of information stored in them.

Note: Information may still be subject to FPT Software Restricted, Confidential, or Internal classification even if it is publicly available elsewhere, where the information is collected, used, or accessed as part of FPT Software business operations. For example, customer name, address and phone number are Confidential even though this information may have been published by the customer.

FPT Software Highly Confidential	
Information category	**Examples** *(Note: This is not an all-inclusive list)*
Sensitive Personally Identifiable Information (SPII) This category includes information which, by itself or in combination, can potentially be used to uniquely identify employees, subscribers, 3rd party workers, and other service parties, including any piece of information which can potentially be used to contact, locate, impersonate, or initiate financial transactions using the identity of a single person. Contact “FHO.GDPR” team in case you have any questions	1. Social Security 2. Government issued ID numbers such as driver license, passport, military ID, etc. 3. Date of birth, religion 4. Payment card information (PCI) – Primary Account Number (PAN) by itself or in combination with one, some or all of the following data items · Cardholder name · Service code · Expiration date · Sensitive authentication data - Full track data (magnetic stripe or equivalent on a chip) - CAV2/CVC2/CVV2/CID numbers - PIN/PIN block Payment cards include credit cards, debit cards or prepaid cards that are branded such as Visa, MasterCard, American Express, etc. Account number in combination with any required security code, access code, or password that would permit access to an individual’s financial account. 5. Password (account password, answers to secret questions or PIN) 6. Location Information: Information to pinpoint or derive the location of the handset or customer. Examples include: a. Cell tower location information

FPT Software Highly Confidential	
Information category	**Examples** *(Note: This is not an all-inclusive list)*
	b. E911 address c. Device latitude/longitude coordinates (which can be derived with a variety of methods) d. IP address (network address) e. Customer location data 7. Customers' behavioral tracking information is information collected from one or more sources to draw conclusions about their interests and can be used to improve ad targeting and marketing results. Examples include: Tracking the number of on-time/late payments to draw conclusions about a customer's financial position Information collected from online cookies to track activities or draw conclusions about their interests from the items clicked or amount of time spent on a webpage 8. Service application, payment history, credit rating, application denial, termination of service, or collections history that are tied to a customer's name or account number 9. Codes on Prepaid phone cards, Google Play, or iTunes cards used in or for business purposes. 10. Employee and candidate information, including: · CVs, skill profile, citizenship or immigration status · Race or ethnicity · Gender and/or sexual orientation · Biometric information such as fingerprints or face ID · Religious affiliation · Criminal history · Records of personal bankruptcy
Customer Proprietary Network Information (CPNI)	Individually identifiable CPNI is restricted and includes: a. Quantity – how often a number is dialed or sent a message b. Configuration – rate plan and features c. Type – mobile to mobile or roaming d. Call/Message Destination – the number called or data sent to e. Location – origin and destination location f. Amount – minutes used or duration of call g. Date & time – when the transmission took place
Customer Created Content	Includes the content of text messages, emails, pictures, address book contacts, and customer marketing communication preference data.

FPT Software Highly Confidential	
Information category	**Examples** *(Note: This is not an all-inclusive list)*
Employee Specific Compensation and Benefit Information, Regulatory Review, Assessment, or Audit Information	Individual's personal wage, bonus, stock information, payroll deductions … 1. Benefit information (life insurance, leave of absence, short-term and long-term disability selections, flexible spending accounts, dependent information, etc.) 2. Employee performance reviews 3. OFCCP (Office of Federal Contract Compliance Programs) reports, reviews, and audit findings (applicable in the US) 4. Equal Employment Opportunity Commission reviews and findings
Protected Health Information (PHI)	1. Past, present, or future medical conditions or mental health information 2. Medical records, medical/insurance billing, data 3. Medical claim forms, medical payments and copayments, health plan enrollment, disenrollment, and maintenance data
Operational Information requiring the highest level of protection	Highly sensitive competitive or strategic information: 1. Unpublished or future prices, fee schedules, pricing policies or formulas, or marketing plans or strategies 2. Unpublished future product offerings, service plans, release dates 3. Future profit margins or profitability targets on specific services or products 4. Trade secrets, unfiled patents 5. Technical and design drawings depicting Company's proprietary technologies 6. Current or future network planning strategies (e.g., deployment of new facilities and technologies, detailed tower locations, and capacity utilization or constraints) 7. Customer or prospective customer lists, prospective bidding plans, or detailed information about pending bids 8. Detailed cost information about individual products or services and intentions to bid or not bid for specific customers or products 9. Attorney-client privilege information 10. Audit findings, incident reports and investigation information 11. Unpublished financial reports and financial information, both historic and projected, prior to public disclosure 12. Any information related to a merger or acquisition and/or related to a spectrum auction 13. System vulnerability, risk /vulnerability assessments, and risk findings/exceptions/remediation plans

FPT Software Highly Confidential	
Information category	**Examples** *(Note: This is not an all-inclusive list)*
	14. Security risk assessments/reports/repositories which contain information about security/privacy gaps and findings. 15. Encryption keys including private digital signature keys. 16. IT technical and operational information a. Authentication credentials – e.g., usernames in combination with passwords, answers to secret questions, certificates, private keys, tokens etc. b. Sensitive IT project information (e.g., IP address, qualified domain names, detailed network /architectural diagrams, host names, network segmentation, etc.) c. Detailed device and system configuration d. Computer program source code and system design documentation 17. Board and management meeting minutes
Personally identifiable information (PII)	Information which can, or when combined can, potentially be used to uniquely identify a person or entity. 1. Full Name or first initial and last name in combination with a listed or implied descriptive characteristic, e.g., names of FPT Software customers. 2. Telephone number/MSISDN/ Billing Account Number (BAN), IMEI/IMSEI Address (email/ postal address) of a customer, employee, supplier or other party. 3. Tax ID (EIN or ITIN or other terms used in applicable laws) 4. Bank ABA routing number in combination with account number and name (associated with PII)
Employment Information	1. Aggregate or general demographic employee data 2. specific wage/salary 3. EEOC demographic data 4. OFCCP demographic data 5. Candidate PII and background check information gathered during the application process 6. Employee Stock Purchase Plan enrollment status 7. Employee stock grants 8. 401K participation information (applicable in the US) 9. Rehire eligibility 10. Termination reason 11. Aggregate Benefit enrollment information

FPT Software Highly Confidential	
Information category	**Examples** *(Note: This is not an all-inclusive list)*
Operational Information requiring a high level of protection	1. Computer systems and IT management information (to the extent it does not involve competitively sensitive materials which are classified as Restricted – e.g., pricing, network planning, selling strategies) 2. Description of regulatory compliance – means by which the FPT Software meets compliance obligations is proprietary, non-public information. It is in most cases legal advice for how FPT Software should comply and in some instances is elevated to restricted privileged information. 3. Draft press releases and other draft unpublished public relations documents 4. Configuration information for 911 systems 5. Disaster recovery plans 6. IT Technical and Operational Information a. Device and system configuration information b. Reference design – HLSD (High level solution design) documentation c. High level architecture diagrams with no detail about systems, ports, services and protocol addressing schemes 7. De-identified information that cannot be used to personally identify an individual a. Demographic data purchased from third parties b. Aggregate information shared with third parties 8. Aggregate information used during business processes that may have competitive intelligence value (e.g. customer Employer Identification Numbers [EIN] in aggregate)
Information on internal COMPANY sites	1. Contact information in Outlook (Global Address Book), Skype for Business, or Teams 2. General information published on enterprise portals or intranets. 3. Training that is approved and labeled for “Internal” use 4. Detailed non-public job descriptions 5. Bonus plan 6. Organizational charts
Operational Information requiring adequate or moderate level of protection	1. Physical descriptions of existing offices and facilities not currently available to general public 2. Internal posters, flyers and training materials 3. Policy documents as applicable 4. Other operational information for business purposes that does not fall in the categories of Confidential or Restricted

FPT Software Highly Confidential	
Information category	**Examples** *(Note: This is not an all-inclusive list)*
Customers' publicly available information	Information that the customers themselves make public such as inputs on online forums and publicly viewable by others
Information that HR has approved and officially released to the public	Percent of employees participating in Red Cross blood drive programs Press releases about employee participation in volunteer job postings publicly available
Information that has been explicitly approved by the appropriate department (e.g. Media Relations, Government Affairs, and Corporate Communications, Investor relations) as suitable for public view and use	Press releases, marketing brochures, coverage maps, and public information on the FPT Software websites

2.4 Information Degrade

Information during its lifecycle may need to be degraded based on the timeframe, audience, and other requirements. These requirements will be set by the Information Owner and communicated to those with a need-to-know.

3 APPENDIXES

3.1 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
Information Rating	All information will be marked or annotated to assist with processing, distribution, storage and disposal. Information classification marks are: "top secret information" and "confidential information" should be placed at the bottom of all the files in the central (if practicable). If the information

Abbreviations	Description
	classification mark is not visible, it can be embedded in the metadata of the file. all information will be classified according to the following classification labels: • Top Secret Information ("Top Secret Information ") • Confidential Information ("Confidential Information ") • Internal use (Only internal information for employees) Public information
DPO/GDPO	Data Protection Officer/Global Data Protection Officer
DPIA	Data Protection Impacted Assessment
PIMS	Personal Information Management System
EU	European Union

3.2 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 Sept. 30, 2011
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
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

No	Code	Name of documents
18	PDPA Thailand	Thailand's Personal Data Protection Act, 06/2022
19	PDPA Malaysia	Personal Data Protection Act 2010, Malaysia
20	TISAX	Trusted information security assessment exchange
21	BS10012: 2017	British Standard Personal Information Management System
22		Vietnamese laws on Privacy: - Article 21 of the 2013 Constitution - Article 38 of the Civil Code 2015 - Article 125 of the Penal Code - Clause 2 of Article 19 of the Labor Code Decree of the Vietnamese Government: Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân Came in force 07/2023
23	FPT Software Personal Data Protection Handbook	PDP_ Handbook_Version_V3.4

3.3 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.

3.4 Example PII: