



## *Policy*

# **PRIVACY STATEMENT**

<b>Document Code</b>	<b>16e-HD/SG/HDCV/FSOFT</b>
<b>Version</b>	<b>1.3.1</b>
<b>Effective date</b>	<b>14-May-2024</b>

**TABLE OF CONTENT**

1 INTRODUCTION .....	4
1.1 Purpose .....	5
1.2 Application Scope .....	5
1.3 Application of national Laws .....	5
1.4 Responsibilities .....	6
2 PRIVACY STATEMENT .....	7
2.1 Document Owner and Approval .....	12
3 APPENDIX .....	13
3.1 Definition .....	13
3.2 Related Documents .....	14
3.3 Data Protection Law, Vietnam, Overview .....	16

**RECORD OF CHANGE**

No	Effective Date	Version	Change Description	Reason	Reviewer	Final Reviewer	Approver
1	01-Jul-2021	1.0	Newly issued	BS 10012:2017 Requirements/G DPR, Clause 6.1.3.1, 6.1.3.2, 8.2.6.1, 8.2.6.2, 8.2.6.5	Trang	Michael Hering	CFO/COO
2	01-Apr-2022	1.1	1.2 added: (see Guideline_PIMS Scope_v1.1), Contact details, address line 2, Lot T2, D1 St., Tan Phu Ward, Thu Duc City 3.2 13 added: PDPL, UAR, Decree-Law No. 45 of 2021 3.2 15 added: Decree of the Vietnamese Government: Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân 3.2 16 PDP_Handbook_Version_V3.2	Biannually revision	Linh Do Thi Dieu	Michael Hering	CFO/COO
3	01-Nov-2022	1.2	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
4	01-Aug-2023		Changed email to <a href="mailto:michael.hering@fpt.com">michael.hering@fpt.com</a> Adjust document version numbers added 3.2 14, 18 changed 3.2 22: Came in force 07/2023 changed 4.3 PDPD was finalized and was coming in force 07/2023	Biannually revision	Linh Do Thi Dieu	Michael Hering	CFO/COO
5	14-May-2024		change document classification, from 'internal use' to 'public'	Document classification	Linh Do Thi Dieu	Michael Hering	CFO/COO

## 1 INTRODUCTION

FPT Software Company, Ltd. ("FPT Software" hereinafter) Corporate Data Protection Policy, privacy statement, procedures, guidelines, 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, privacy statement, procedures, 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, legal entities, and partners. FPT Software have established guiding data protection principles – among them transparency, data economy and data security – as FPT Software guidelines.

## **1.1 Purpose**

The FPT Software Personal Data Handbook including the Protection Policy, Policy\_Personal Data Protection Management\_v3.4 and privacy statement applies worldwide to FPT Software, Subsidiaries as well legal entities and is based on globally accepted, basic principles on data protection. Ensuring data protection is the foundation of trustworthy business relationships and the reputation of the FPT Software as a first-class employer.

The Data Protection Policy provides one of the necessary framework conditions for cross-border data transfer among FPT Software, Subsidiaries, and legal entities. It ensures the adequate level of data protection prescribed by the European Union General Data Protection Regulation, APPI, PDPA or other national Personal Data Protection Regulations and the national laws for cross-border data transmission, including in countries that do not yet have adequate data protection laws.

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 the personal data protection management policy, Data Protection Handbook, Privacy Statement, and information security policies.

## **1.2 Application Scope**

All processing of personal data by FPT Software is within the scope of this procedure.

Means, all FPT Software's business processes and information systems involved in the collection, processing, use and transfer of personal data and all employees, contractors and 3<sup>rd</sup> party providers involved in the processing of personal data on behalf of FPT Software.

This policy 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 procedure.

In scope are all data subjects whose personal data is collected, in line with the requirements of the GDPR and other national/international data protection regulation (see Policy\_PIMS Scope\_v1.3.1).

## **1.3 Application of national Laws**

The Data Protection Policy, privacy statement, procedures, guidelines, and templates comprise 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, procedures 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 privacy statement, guidelines, and the legal obligations. If there is reason to believe that legal obligations contradict the duties under the Data Protection Policy, privacy statement, procedures

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 privacy statement, FPT Software 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, guidelines, and this procedure.

#### **1.4 Responsibilities**

The Global Data Protection Officer is responsible for ensuring that the privacy statement is correct and that mechanisms exist such as having the privacy statement on FPT Software website to make all data subjects aware of the contents of this notice prior FPT Software commencing collection of their data.

The Global Data Protection Officer is responsible for ensuring that this statement is made available to data subjects prior to FPT Software collecting/processing their personal data.

All Employees/Staff of FPT Software who interact with data subjects are responsible for ensuring that this statement is drawn to the data subject's attention and their consent to the processing of their data is secured.

## 2 PRIVACY STATEMENT

FPT Software is part of FPT Corporation (FPT – HoSE) – the global leading technology and IT services group headquartered in Vietnam with nearly US\$1.2 billion in revenue and 30,000 employees. Qualified with CMMI Level 5 & ISO 27001:2013, ASPICE LEVEL 3, FPT Software delivers world-class services in Smart factory, Digital platform, RPA, AI, IoT, Enterprise Mobilization, Cloud, AR/VR, Embedded System, Managed service, Testing, Platform modernization, Business Applications, Application Service, BPO and more services globally from delivery centers across the United States, Japan, Europe, Australia, Vietnam and the Asia Pacific.

<b>Personal data type:</b>	<b>Source</b> (FPT Software obtained the personal data from if it has not been collected directly from you, the data subject.
name, email address, designation, company, country and telephone number	FPT Software WEB page
IP address, demographics, your device operating system, and browser type	FPT Software WEB page

### Personal Information we may collect and process

You can access or visit our website at any time without informing us who you are or providing us any personal information. However, we may collect information at our websites in two ways: (1) directly (for example, when you provide information, such as your name, email address, designation, company, country and telephone number, to sign up for a newsletter or register to comment on a forum website); and (2) indirectly (for example, through our website's technology, we may collect certain information such as your IP address, demographics, your computers' operating system, and browser type). We do not attempt to track your personal information in order to identify you, but gathering these contact information in order to make up the web traffic routing, to diagnose problems with server for administration of our website, to better understand how you interact with our website and services and to re-design and upgrade the website for better use. If you choose not to provide your personal information that is mandatory to process your request, we may not be able to provide the corresponding service.

**Use of collected information**

We use personal data to provide you with information you request, process online job applications, and for other purposes which we would describe to you at the point where it is collected or which will be obvious to you. For example:

- To further fulfill your requirements on products and services
- To contact you with the aim of developing a business relationship
- To feedback to your idea and/or to provide you relevant information at your requirements
- To contact you for marketing purpose such as customer surveys.
- To inform you about our company
- To obey regulations in applicable laws

**Consent**

By consenting to this privacy notice you are giving us permission to process your personal data specifically for the purposes identified.

Consent is required for FPT Software to process personal data, but it must be explicitly given. Where we are asking you for personal data, we will always tell you why and how the information will be used.

You may withdraw consent at any time by email, a written letter or telephone call to our Global Data Protection Officer or local subsidiary in line with our Procedure Withdrawal of Consent (procedure\_withdrawal consent\_V1.3. Retrieve a copy of guideline and procedure Global Data Protection Officer).

**Data recipients, transfer, and disclosure of personal information:**

We do not share your personal information with third parties without seeking your prior permission. We will seek your consent prior to using or sharing personal information for any purpose beyond the requirement for which it was originally collected. However, we may share your personal information within FPT Software or with any of its subsidiaries, business partners, service vendors, authorized third-party agents, or contractors located in any part of the world for the purposes of data processing, storage, or to provide a requested service or transaction, after ensuring that such entities are contractually bound by data privacy obligations. When required, we may disclose personal information to external law enforcement bodies or regulatory authorities, in order to comply with legal obligations. We do not intend for our websites or online services to be used by anyone under the age of 13. If you are a parent or guardian and believe we may have collected information about a child, please contact us as described in this Privacy Statement.

**Disclosure**

FPT Software will pass on your personal data to third parties.



<b>Third country (non-EU)/international organisation</b>	<b>Safeguards in place to protect your personal data</b>	<b>Retrieve a copy of the safeguards in place here:</b>
FPT Software subsidiaries and legal entities globally	Processing agreement including Standard Contract Clause	Global Data Protection Officer

### **Retention period**

FPT Software will process personal data for one year. Retention period 2 years or based on applicable national laws/regulations (reference: Guideline\_Personal Data Retention\_v3.4.1, Procedure\_Retention of Records\_V1.3.1. Retrieve a copy of guideline and procedure Global Data Protection Officer).

### **Cookies policy**

Like many websites, when you access to our websites, we will use “website assessment diary”- a cookie technology to collect additional website usage data. A cookie is a small data file that we transfer to your computer to facilitate your assessment to our websites. We may use information collected from our cookies to identify user behavior and to serve content and offers based on your profile, and for the other purposes described below, to the extent legally permissible in certain jurisdictions. In addition, when you visit our websites, our advertisement partners, whom we have engaged for re-marketing, may introduce cookies. Based on your browsing of our website you may see our advertisements while browsing through our advertisement partner websites and/or their network websites. Such cookies would allow us to monitor the effectiveness of the advertisements and to make the advertisements more relevant to you. By using our site, you agree that we can place cookies on your device as explained herein. If you want to remove existing cookies from your device, you can do this using your browser options. Most Internet browsers automatically accept cookies. You can instruct your browser, by editing its options, to stop accepting cookies or to prompt you before accepting a cookie from the websites you visit.

### **Data Security**

FPT Software commits to secure your personal information with securities measures in place. The measures will help protecting data from the misuse, loss, leakage and/or alteration of information. Your personal information is access restricted to authorize FPT Software’s personnel for the sake of providing service at your requirements and/or for FPT Software’s audit, internal audit and for the purpose of law obligation. We strictly require our personnel, in any way, to protect your personal information and have use all measurements, technology and recognized security process for this purpose in compliance with government authorizations’ regulations. Regarding your use of our websites you should understand that the open nature of the Internet is such that information and personal data may flow over networks connecting you to our systems without security measures and may be accessed and used by people other than those for whom the data is intended.

### **Links to other websites**

This site contains links to other websites, but they are neither FPT Software's websites nor under control of FPT Software. FPT Software is not responsible for the privacy practices or the content and transactions of such websites. You are required to read carefully the Privacy part of those linked websites to assure that you have fully understood the way of personal information collection and sharing before providing your own information. You shall take all responsibility of risk that may incur when using those websites.

### **Your rights as a data subject**

At any point while we are in possession of or processing your personal data, you, the data subject, have the following rights:

- Right of access – you have the right to request a copy of the information that we hold about you.
- Right of rectification – you have a right to correct data that we hold about you that is inaccurate or incomplete.
- Right to be forgotten – in certain circumstances you can ask for the data we hold about you to be erased from our records.
- Right to restriction of processing – where certain conditions apply to have a right to restrict the processing.
- Right of portability – you have the right to have the data we hold about you transferred to another organisation.
- Right to object – you have the right to object to certain types of processing such as direct marketing.
- Right to object to automated processing, including profiling – you also have the right to be subject to the legal effects of automated processing or profiling.
- Right to judicial review: if FPT Software refuses your request under rights of access, we will provide you with a reason as to why. You have the right to complain as outlined in below.

All the above requests will be forwarded on should there be a third party involved in the processing of your personal data.

FPT Software accepts the following forms of ID when information on your personal data or data subject rights are requested:

Passport, driving licence, ID card

## Complaints

If you wish to make a complaint about how your personal data is being processed by FPT Software or how your complaint has been handled, you have the right to lodge a complaint directly with the supervisory authority and FPT Software's data protection representatives Global Data Protection Officer.

### Contact details:

	<b>Supervisory authority contact details</b>	<b>Data Protection Officer (DPO), Data Protection Representatives</b>
Contact Name:	Andrea Vosshoff, Federal Commissioner for Freedom of Information	Michael Hering, Global Data Protection Officer
Address line 1:	Husarenstraße 30	F-Town Building 3, Saigon Hi-Tech Park,
Address line 2:	53117 Bonn	Lot T2, D1 St., Tan Phu Ward, Thu Duc City
Address line 3:	Germany	HCM City, Vietnam
Email:	<a href="mailto:poststelle@bfdi.bund.de">poststelle@bfdi.bund.de</a>	michael.hering@fpt.com
Telephone:	+49 228 997799 0; +49 228 81995 0	+84 902606236

## Changes on Privacy Statements

FPT Software reserves the rights to change, modify, add or remove in whole or in part this Privacy Statement at its sole discretion, at any time. Therefore, you are responsible for regularly reviewing this statement. Changes of this Privacy Statements will be posted on this website. These changes will also be effective when they are posted. Your continued use of this statement constitutes your agreement to all such terms.

## Contact

If you have any questions about our Privacy Statement or about how to protect your personal information, you can contact the Global Data Protection Officer of FPT Software or every local subsidiary of FPT Software.

Global Data Protection Officer:

Michael Hering, michael.hering@fpt.com, +84 902606236,  
F-Town Building 3, Saigon Hi-Tech Park, Lot T2, D1 St., Tan Phu Ward, Thu Duc City, HCM City, Vietnam

## **2.1 Document Owner and Approval**

The Data Protection Officer (GDPO) is the owner of this document and is responsible for ensuring that this statement is reviewed in line with the review requirements of the GDPR and Guideline\_Personal Data Protection Policy Development\_v2.4.1.

This statement was approved by the CFO, board member responsible for data protection, see record of change.

### 3 APPENDIX

#### 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
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		<p>Vietnamese laws on Privacy:</p> <ul style="list-style-type: none"> <li>- Article 21 of the 2013 Constitution</li> <li>- Article 38 of the Civil Code 2015</li> <li>- Article 125 of the Penal Code</li> <li>- Clause 2 of Article 19 of the Labor Code</li> </ul> <p>Decree of the Vietnamese Government:            Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân            Came in force 07/2023</p>
23	FPT Software Personal Data Protection Handbook	PDP_ Handbook_Version_V3.4.1

### 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/QĐ-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.