Procedure

PRIVACY

Document Code	10e-QT/SG/HDCV/FSOFT
Version	1.4
Effective date	01-Dec-2024

TABLE OF CONTENT

RECORD OF CHANGE

No	Effective Date	Version	Reason	Change Description	Reviewer Local DPO VN	Final Reviewer GDPO	Approver
1	01-Jul-2021	1.0	Newly issued	BS 10012:2017 Requirements/GDPR, 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	Biannually revision	1.1 changed: Policy_Personal Data Protection Management_v3.2 1.2 added: Policy_PIMS Scope_v1.1 2.2 13 added PIPL, 2.2 14 added: PDPL, UAR, Decree-Law No. 45 of 2021 2.2 16 added: Decree of the Vietnamese Government: Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân 2.2 17 PDP_ Handbook_Version_V3.2 2.2 18: 15e-HD/SG/HDCV/FSOFT	Linh Do Thi Dieu	Michael Hering	CFO/COO
3	01-Nov-2022	1.2	Biannually revision	Added 2.3. Data Protection Law, Vietnam, Overview. Added 2.2 15 Republic Act 10173 Data privacy Act 2012 Added 2.2 16 PIPL Added 2.2 17 PDPA Added 2.2 18 TISAX	Linh Do Thi Dieu	Michael Hering	CFO/COO
4	01-Aug-2023	1.3	Biannually revision	Adjust document version numbers added 2.2 14, 18 changed 2.2 22: Came in force 07/2023 changed 2.3 PDPD was finalized and was coming in force 07/2023	Linh Do Thi Dieu	Michael Hering	CFO/COO
5	14-May-2024	1.3.1	Document classification	change document classification, from 'internal use' to 'public'	Linh Do Thi Dieu	Michael Hering	CFO/COO
6	01-Dec-2024	1.4	Biannually revision	Added 1., 1.1 PDPD13, Added 4.2 20, 4.2 24 Changed 4.2 7 to March 15, 2024	Linh Do Thi Dieu	Michael Hering	CFO/COO

1 INTRODUCTION

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

The General Data Protection Regulation (GDPR), PDPD13 defines “personal data” as 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.

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).

1.1 Purpose

The Data Protection Policy/Privacy Statement Policy_Personal Data Protection Management_v3.5 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, PDPD13 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 Name 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 3rd party providers involved in the processing of personal data on behalf of FPT Software.

This procedure 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. See Policy_PIMS Scope_v1.4.

1.3 Application of national Laws

The Data Protection Policy, procedures, 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, 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 guideline and the legal obligations. If there is reason to believe that legal obligations contradict the duties under the Data Protection Policy, 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 guideline, 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 Data Protection Policy and the privacy statement is correct and that mechanisms exist such as having the Data Protection Policy and 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.

1.5 Procedure Article 12

FPT Software identifies the legal basis for processing personal data before any processing operations take place by clearly establishing, defining, and documenting:

The specific purpose of processing the personal data and the legal basis to process the data under:

Consent obtained from the data subject

Performance of a contract where the data subject is a party

Legal obligation that FPT Software is required to meet

Protect the vital interests of the data subject, including the protection of rights and freedoms

Necessary for the legitimate interests of the data controller or third party, unless the processing is overridden by the vital interests, including rights and freedoms

National law

Any special categories of personal data processed and the legal basis to process the data under:

Explicit consent obtained from the data subject

Necessary for employment rights or obligations

Protect the vital interests of the data subject, including the protection of rights and freedoms

Necessary for the legitimate activities with appropriate safeguards

Personal data made public by the data subject

Legal claims

Substantial public interest

Preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, provision of health or social care treatment, or management of health and social care systems and services, under the basis that appropriate contracts with health professionals and safeguards are in place

Public health, ensuring appropriate safeguards are in place for the protection of rights and Freedoms of the data subject, or professional secrecy

National laws in terms of processing genetic, biometric or health data

FPT Software records this information in line with its data protection impact assessment (Guideline_Risk Management_DPIA_v2.5) and data inventory (Guideline_Personal Data Inventory Management_v3.5).

1.6 Privacy Statement

When personal data collected from data subject with consent:

FPT Software is transparent in its processing of personal data and provides the data subject with the following:

FPT Software's identity, and contact details of the Global Data Protection Officer and any local data protection representatives

The purpose(s), including legal basis, for the intended processing of personal data

Where relevant, FPT Software's legitimate interests that provide the legal basis for the processing

Potential recipients of personal data

Any information regarding the intention to disclose personal data to third parties and whether it is transferred outside the EU. In such circumstances, FPT Software will provide information on the safeguards in place and how the data subject can also obtain a copy of these safeguards

As FPT Software is based outside of the EU and the data subject resides within it (the EU), FPT Software provides the data subject with contact details of a local data protection representative in the EU

Any information on website technologies used to collect personal data about the data subject

Any other information required to demonstrate that the processing is fair and transparent (Policy_Personal Data Protection Management_v3.5, Guideline_Complaints and Appeals Handling_v3.5, Template_Data Subject Right Request Form_v2.5).

All information provided to the data subject is in an easily accessible format (email, WEB page, printed letter), using clear and plain language, especially for personal data addressed to a child.

FPT Software facilitates the data subject's rights in line with the data protection policy (Policy_Personal Data Protection Management_v3.5) and the subject access request procedure (Procedure_Data Subject Access Request_v1.4).

Privacy statement for personal data processing is recorded (FPT Software WEB page, Policy_Privacy Statement_v1.4)

When data is contractually required for processing:

FPT Software processes data without consent in order to fulfil contractual obligations

Privacy notice for this personal data processing is recorded (FPT Software WEB page, Policy_Privacy Statement_v1.4)

When personal data has been obtained from a source other than the data subject, FPT Software makes clear the types of information collected as well as the source of the personal data (publicly accessible sources) and provides the data subject with:

FPT Software's (data controller) identity, and contact details of the Global Data Protection Officer and any local data protection representatives

The purpose(s), including legal basis, for the intended processing of personal data

Categories of personal data

Potential recipients of personal data

Any information regarding disclosing personal data to third parties and whether it is transferred outside the EU – FPT Software will provide information on the safeguards in place and how the data subject can also obtain a copy of these safeguards

Any other information required to demonstrate that the processing is fair and transparent (Guideline_Personal Data Retention_v3.5, Procedure_Retention of Records_v1.4, Guideline_Complaints and Appeals Handling_v3.5).
Privacy notice for this personal data processing is recorded (FPT Software WEB page, Policy_Privacy Statement_v1.4)

FPT Software provides the information stated above within:

One month of obtaining the personal data, in accordance with the specific circumstances of the processing

At the first instance of communicating in circumstances where the personal data is used to communicate with the data subject

When personal data is first disclosed in circumstances where the personal data is disclosed to another recipient

Above do not apply:

If the data subject already has the information

If the provision of the above information proves impossible or would involve an excessive effort (GDPR provides additional clarity where the purpose of processing for archiving information in the public interest, scientific or historical research purposes, or statistical purposes. In these instances, it may be the case that making disclosures “render impossible or seriously impair the achievement of the objectives of that processing”. If this is the case, the FPT Software will apply appropriate measures to protect the data subject’s rights and freedoms)

If obtaining or disclosure of personal data is expressly identified by Member State law

If personal data must remain confidential subject to an obligation of professional secrecy regulated by Member State law, including a statutory obligation of secrecy

1.7 Document Owner and Approval

The Data Protection Officer (GDPO) is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the GDPR and Guideline_Personal Data Protection Policy Development_v2.5.

A current version of this document is available and published to FPT Software employees on QMS.

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

2 APPENDIX

2.1 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

2.2 *Related Documents*

No	Code	Name of documents
1	EU GDPR/GDPR UK	EU General Data Protection Regulation/UK
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
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	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	ISO 27001	Information security, cybersecurity and privacy protection — Information security management systems
24	ISO 27701	ISO/IEC 27701:2019 (formerly known as ISO/IEC 27552 during the drafting period) is a privacy extension to ISO/IEC 27001. The design goal is to enhance the existing Information Security Management System (ISMS) with additional requirements in order to establish, implement, maintain, and continually improve a Privacy Information Management System (PIMS). The standard outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage privacy controls to reduce the risk to the privacy rights of individuals.
25	PDPD13, VN	Decree of the Vietnamese Government: PDPD13 Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân 07/2023
26	FPT Software Personal Data Protection Handbook	PDP_ Handbook_Version_V3.5

2.3 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.