



Procedure

**DATA PROTECTION
MANAGEMENT REVIEW**

Document Code	18e-QT/SG/HDCV/FSOFT
Version	1.3
Effective date	01-Aug-2023

TABLE OF CONTENT

1 INTRODUCTION 4

 1.1 Purpose 4

 1.2 Application Scope 5

 1.3 Application of national Laws 5

 1.4 Responsibilities 6

2 Management Review Inputs 7

3 Management Review Outputs 9

4 Document Owner and Approval 11

5 APPENDIX 12

 5.1 Definition 12

 5.2 Related Documents 13

 5.3 Data Protection Law, Vietnam, Overview 15

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/GDPR, Clause 9.3	Nguyen Ngoc Trang	Michael Hering	HoanNK
2	01-Apr-2022	1.1	Biannually revision	1.2 added: Policy_PIMS Scope_v1.1 5.2 13 added PIPL, 5.2 14 added: PDPL, UAR, Decree-Law No. 45 of 2021 5.2 16 added: Decree of the Vietnamese Government: Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân 5.2 17 PDP_ Handbook_Version_V3.2 5.2 18: 15e-HD/SG/HDCV/FSOFT	LinhDTD1	Michael Hering	HoanNK
3	01-Nov-2022	1.2	Biannually revision	Added 5.3. Data Protection Law, Vietnam, Overview. Added 5.2 15 Republic Act 10173 Data privacy Act 2012 Added 5.2 16 PIPL Added 3.2 17 PDPA Added 5.2 18 TISAX	LinhDTD1	Michael Hering	HoanNK
4	01-Aug-2023	1.3	Biannually revision	Adjust document version numbers added 5.2 14, 18 changed 5.2 22: Came in force 07/2023 changed 5.3 PDPD was finalized and was coming in force 07/2023	LinhDTD1	Michael Hering	HoanNK

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.

1.1 Purpose

The FPT Software Personal Data Handbook including the Protection Policy, Policy_Personal Data Protection Management_v3.4 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 an adequate level of data protection prescribed by the European Union General Data Protection Regulation, APPI, PDPA and other national Personal Data Protection Regulations and national laws for cross-border data transmission, including to countries that do not have adequate data protection laws, yet.

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

The Data Protection Policy (Policy_Personal Data Protection Management_v3.4) and Personal Data Protection arrangements (data protection handbook including policies, procedures, guidelines, records, templates) are subject to development, review, evaluation and continuous improvement.

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 are in scope.

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_v1.3.

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, who is the defined owner of the Data Protection Policy, is responsible for its development, review and evaluation.

The Head of ISM (Information Security Management) who is the defined owner of the Information Security Policy, is responsible for its development, review and evaluation.

The designated FPT Software Board member for Data Protection and the designated FPT Software Board member for Information Security is responsible for carrying out reviews in line with this procedure and for driving compliance to the GDPR, APPI, PDPA and other national Personal Data Protection Regulations.

The Head of IT is responsible for convening meetings of the Head of ISM, GDPO, designated FPT Software Board member for Data Protection and designated FPT Software Board member for Information Security either after there have been (or it is planned that there will be) significant changes in the organizational environment, business circumstances, legal conditions or technical environment, and which is likely to have an impact on the level of risk facing personal data, or at least annually.

The Global Data Protection Officer of is responsible for the application and effective working of this procedure.

2 Management Review Inputs

Management reviews must consider:

Status of actions from previous management reviews

Changes in internal and external issues (e.g., Codes of Conduct) relevant to the GDPR, APPI, PDPA and other national Personal Data Protection Regulations.

Information on GDPR, APPI, PDPA and other national Personal Data Protection Regulations performance including trends in:

- Nonconformities and corrective actions
- Monitoring and measurement evaluation results
- Internal and external audit reports
- Results and/or trends from the measurement of progress towards the protection of information security and personal data.

Performance for GDPR, APPI, PDPA and other national Personal Data Protection Regulations compliance must be considered, including:

- Follow-up actions from previous management reviews
- Need for changes including its policy and objectives
- Opportunities for improvement
- Results of audits, reviews, DPIA, data inventory
- Results of audits and reviews of key suppliers and partners
- Techniques, products or services which could be used to improve compliance with the GDPR
- Status of corrective actions
- Results of exercises and tests
- Risks or issues not adequately addressed
- Changes (internal or external) that could affect compliance with GDPR, APPI, PDPA and other national Personal Data Protection Regulations
- Adequacy of Data Protection Policy and Personal Data Protection Handbook
- Recommendations for improvement (internally or externally generated)
- Complains, appeals, data subject right request
- Data protection incidents
- Lessons learned

- Actions arising from disruptive incidents (post-incident reports)
- Emerging good practice and guidance

3 Management Review Outputs

Improving FPT Software's assessment of the risks, including updating the risk assessment and incident management plans

Any variations to the scope of the GDPR, APPI, PDPA and other national Personal Data Protection Regulations that may be required.

Modifying or improving the policies and procedures and their effectiveness, ensuring that any changes to business or business processes, or changes to statutory, regulatory or contractual requirements are accommodated

Update of risk assessments, plans and related procedures

Modification of procedures and controls to respond to internal or external events that may impact compliance with the GDPR, APPI, PDPA and other national Personal Data Protection Regulation, including changes to:

- Business and operational requirements
- Risk reduction and security requirements
- Operational conditions and processes
- Legal and regulatory requirements
- Contractual obligations
- Levels of risk; criteria for accepting risks
- Resource needs
- Funding and budget requirements

Reviewing and improving how the effectiveness of controls is measured

Improving the allocation of resources and responsibilities, including ensuring that complying with the GDPR, APPI, PDPA and other national Personal Data Protection Regulations is supported by adequate resources, funding and budget.

Formulating and agreeing any changes to the Data Protection Policy which would be necessary to give effect to any improvements identified

The Global Data Protection Officer is responsible for ensuring that the review meeting is recorded and consistent with the GDPR, APPI, PDPA and other national Personal Data Protection Regulations requirements to retain records of reviews, and to review and update processing operations where necessary. The record is signed by its chair, and required actions identified for follow up.

The Global Data Protection Officer is responsible for ensuring that:

- results of management reviews are communicated as appropriate to relevant interested parties
- appropriate actions are taken as a result of management review

The designated Board Member for Data Protection must approve any changes to the policy latest at its next scheduled meeting and prior to its implementation.

4 Document Owner and Approval

The Global 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, other national/international data protection regulations and Guideline_policy_development_V2.4.

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.

5 APPENDIX

5.1 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

5.2 *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"> - 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 <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

5.3 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.