

***Guideline***

**PERSONAL DATA PROTECTION ORGANIZATION**

|  |  |
| --- | --- |
| Document Code | 02e-HD/SG/HDCV/FSOFT |
| Version | 3.3 |
| Effective date | 01-Nov-2022 |

Table of content

[1 introduction 5](#_Toc117583922)

[1.1 Purpose 5](#_Toc117583923)

[1.2 Application Scope 5](#_Toc117583924)

[1.3 Application of national Laws 6](#_Toc117583925)

[2 GUIDELINE CONTENT 7](#_Toc117583926)

[2.1 PIMS Organization Structure 7](#_Toc117583927)

[2.2 Group description and responsibilities 8](#_Toc117583928)

[3 APPENDIXES 12](#_Toc117583929)

[3.1 Definition 12](#_Toc117583930)

[3.2 Related Documents 13](#_Toc117583931)

[3.3 Data Protection Law, Vietnam, Overview 14](#_Toc117583932)

RECORD OF CHANGE

| No | Effective Date | Version | Change Description | Reason | Reviewer | Final Reviewer | Approver |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 10-May-2019 | 1.0 | Newly issued | Legal requirement | MinhPT | Michael Hering | HoanNK |
| 2 | 21-Oct-2019 | 1.1 | Add content of Introduction section:  -Adjust the purpose  -Add new definitions and descriptions of them  -Add related documents  -Section 1.5 Change “responsibility” to “Application of national law”. Instead, the responsibility is described in section 2.2  -Adjust PIMS Organization Structure-Adjust group description and responsibilities | Legal requirement | TrangNN4 | Michael Hering | HoanNK |
| 3 | 11-May-2020 | 2.1 | Update Purpose, Application Scope and Related Documents sub-section | Update according to annually revision requirement | TrangnN4 | Michael Hering | HoanNK |
| 4 | 01-Jul-2020 | 2.1.1 | HITRUST | HITRUST requirement | TrangnN4 | Michael Hering | HoanNK |
| 5 | 19-Oct-2020 | 2.2 | Update section: related document | Legal requirement | TrangnN4 | Michael Hering | HoanNK |
| 6 | 01-May-2021 | 3.0 | Change the document structure.  Update section: Related Document | Legal requirement | TrangnN4 | Michael Hering | HoanNK |
| 7 | 01-Oct-2021 | 3.1 | 1 added: FPT Software Personal Data Protection Handbook and ISM guidelines, 1.2 added: statement\_PIMS scope\_V1.0, 2.2 added: procedures, statements, records, Template\_DPO Job Description\_v1.0, Responsible to manage retention, 3.2 added: Procedure\_Retention of Records\_V1.0 Guideline\_Personal Data Retention\_v3.1 | Legal requirement | TrangnN4 | Michael Hering | HoanNK |
| 8 | 01-Apr-2022 | 3.2 | 1.2 changed to: Policy\_PIMS scope\_V1.1  3.2 14 added PIPL, 3.2 15 added: PDPL, UAR, Decree-Law No. 45 of 2021  3.2 17 added: Decree of the Vietnamese Government:  Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân  3.2 18 PDP\_ Handbook\_Version\_V3.2  3.2 19: 05e-HD/SG/HDCV/FSOFT | Biannually revision | LinhDTD1 | Michael Hering | HoanNK |
| 9 | 01-Nov-2022 | 3.3 | Updated 2.1 Org. Structure  Added 3.2, 17, PDPA Malaysia, 3.2, 19, (still not in force) Added 3.3 Data Protection Law, Vietnam, Overview.  Added 3.2 15 Republic Act 10173  Data privacy Act 2012 | TISAX requirements, biannually revision | LinhDTD1 | Michael Hering | HoanNK |

# introduction

FPT Software Company, Ltd. ("FPT Software" hereinafter) Corporate Data Protection Policy, 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, guidelines and templates set a globally applicable data protection and security standard for FPT Software and regulates the sharing of information between FPT Software, subsidiaries, and legal entities. FPT Software have established guiding data protection principles – among them transparency, data economy and data security – as FPT Software Personal Data Protection Handbook and ISM guidelines.

## Purpose

This Data Protection Organization 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 and a first-class service provider.

The Data Protection Organization provides one of the necessary framework conditions for Personal Data processing and 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.

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 the personal data protection organization.

Description of personal data protection governance and the contribution of FPT Software’s board to the protection of personal data and data subject rights by securing the efficiency of the Personal Information Management System (hereinafter PIMS).

## Application Scope

See statement\_PIMS scope\_V1.2.

## 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.

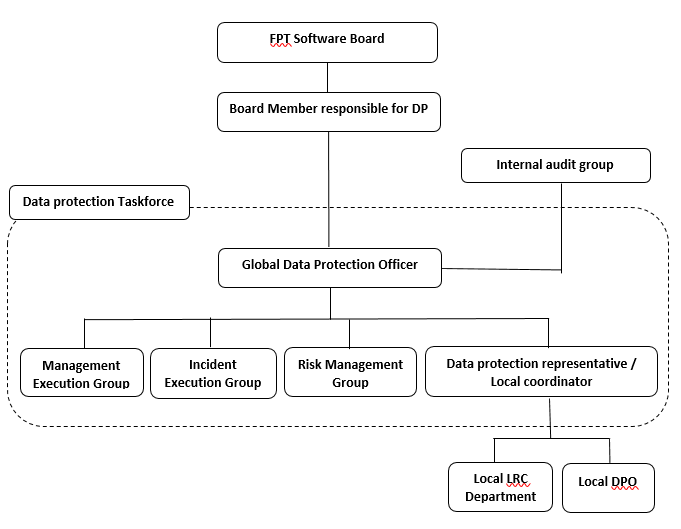
Each subsidiary or legal entity of FPT Software is responsible for compliance with the Data Protection Policy, this guideline, and the legal obligations. If there is reason to believe that legal obligations contradict the duties under the Data Protection Policy or the guidelines, the relevant subsidiary 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 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.

# GUIDELINE CONTENT

## PIMS Organization Structure

FPT Software has implemented a strong governance for Personal Data Protection and PIMS management. Clear roles and responsibilities are defined for PIMS operations, coordination, support of personal data protection, breach/incident management, risk management and DPIA’s.

**Personal Data Protection Organization and Governance**



## Group description and responsibilities

### *FPT Software Board:* C-level management of FPT Software. The highest decision-making level for PIMS. Ensures sufficient manpower, resources, and budget to operate the PIMS framework. Appointing the board member responsible for Personal Data Protection.

### *Board member responsible for DP:* Appointed by the FPT Software CEO.

#### Appointing the Global Data Protection Officer on behalf of the FPT Software CEO.

#### Provide sufficient manpower, resources, and budget on behalf of the FPT Software Board for the GDPO.

#### Approve personal data protection management policies, guidelines, procedures, statements, records, and templates on behalf of the FPT Software Board twice a year.

### *Responsibilities*

### *Global Data*

### *Protection Officer:* Appointed by Board member responsible for DP on behalf of the FPT Software Board, direct report to Board member responsible for DP and member of LRC (Legal, Risk and Compliance). Act as the Data Protection Officer (DPO) of the FPT Software in accordance with laws and regulations. As an obliged organ, its contact information must be submitted to the relevant authorities.

### A data protection officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR), PDPA and other Personal Data Protection Regulations. See Template\_DPO Job Description\_v1.2.

### Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

### The primary role of the DPO is to ensure that the organization processes, the personal data of staff, customers, providers, or any other individuals are protected in compliance with the applicable data protection rules. DPO must be able to perform her duties independently.

#### Responsible for compliance of PIMS and business decisions related to personal information.

Responsible for decision-making, management, and supervision of the DP task force.

Development, reviewing and implementation of PIMS policies, procedures, guidelines, statements,and templates operations twice a year.

Responsible to manage retention of documents/data he is owning based on the Procedure\_Retention of Records\_V1.2 and Guideline\_Personal Data Retention\_v3.3 (record\_retention schedule\_V1.0).

Ensure the implementation and execution of the PIMS.

Periodically (annually) review and audit the execution of the PIMS in FPT Software Units, subsidiaries, and legal entities.

Execution and Confirmation of the internal audit and audit results of PIMS and supervision of the improvement measures based on audit findings.

### *Responsibilities of*

### *Internal Audit Group:* Assigned by the GDPO and approved by Board member responsible for DP.

### Execution and management of 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.

### *Responsibilities of Management Execution Group:* Assigned by the GDPO.

### Update, announce and release the PIMS.

### Develop, coordinate, and arrange all kind of Personal Data Protection trainings including exam.

### Planning the PIMS annual education and training courses.

### Perform and deliver the education and training courses and evaluate the effectiveness of the courses.

### Regularly implementation of laws and regulations, compliance management, and regulatory updates.

### Assist the incident management team in handling complaints.

### Providing legal advice regarding Personal Data Protection for FPT Software units and legal entities.

Members 2022, GDPO and Assistant DPO

### *Responsibilities of Incident Management Group:* Assigned by the GDPO.

### Responsible for Data Subject Rights exercise and management procedure.

### Tracking and management of all complaints, appeals and request from data subjects or complaints about FPT Software units.

Responsible for data breach handling.

A data breach of any size is a crisis management situation, which could put an entire business at risk. Data security is not an IT issue, it is a business risk, and breach response should involve people from a number of roles across the business, including legal, commercial, HR, information security, PR, forensic IT and GDPO. Dealing with a data breach will be alien to many of them. Planning for a breach is therefore essential; every business should have in place a breach response plan, and should designate, in advance, a breach response team (incident management team) which can be convened at short notice to deal with the crisis. Understanding the issues that arise in a breach situation, and practicing managing a breach, are essential to effective breach response. Failure to plan and practice increases the regulatory, litigation and reputation risk to the entire business.

Assist FPT Software units in the prevention, adaptation, and processing of personal data Incidents.

Responsible to organize a root cause analysis of the incident and to report it to the GDPO.

### *Responsibilities*

### *Risk Management*

#### *Group:* Assigned by the GDPO. Job responsibilities are: Implementation of a personal data inventory and risk assessment approach DPIA for FPT Software Units.

#### Develop personal information risk assessment methods and train relevant risk assessment personnel. Plan and execute DPIA.

#### Implementation of risk mitigation measures

Members 2022, GDPO, Assistant DPO supported by LRC Department

### *Responsibilities*

### *Department Data*

### *Protection*

### *Representative/*

### *Local coordinator:* Assigned by Unit, confirmed by GDPO.

### Assist GDPO in the implementation of PIMS for the respective FPT Software Units. Ensure the compliance with the Policy Personal Data Protection Management in the daily routine, including high-risk, sensitive and special personal data protection.

#### Operation of the PIMS regarding the respective FPT Software Unit.

#### Ensure the implementation of security and data protection management measures for the respective FPT Software Unit.

#### Consulting in the root cause analysis of incidents or breaches.

Implementation of measures to void further breaches.

#### Tracking and managing of risk mitigation measures for the respective FPT Software Unit.

#### In of case a personal data protection incident or breach in respective FPT Software Unit, responsible for the root cause analysis and the reporting to the Incident Management Group. Collaborates with Incident Management Group to handle personal data incidents which occur in the respective FPT Software Unit.

Registered Local DPO: DPO Germany/Slovakia, DPO Singapore, DPO Philippines (legally required)

Local Coordination FHM, LRC Team FHM   
Local Coordination FHN, LRC Team FHN   
Local Coordination FDN, LRC Team FDN  
Local Coordination Japan, LRC Team Japan and ISM Team Japan  
Local Coordination FAM, LRC Team FAM  
Subsidiaries and legal entities which do not have a Local DPO or a local LRC team, the Personal Data Protection coordination is a responsibility of the Head of the Unit.

# APPENDIXES

## 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 |

## 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 | PDPL, UAR | Decree-Law No. 45 of 2021 |
| 15 | DPA Philippines | Republic Act 10173, Data privacy Act 2012 |
| 16 | PIPL | Personal Information Protection Law of the People’s Republic of China and related laws and regulations |
| 17 | PDPA Malaysia | Personal Data Protection Act 2010, Malaysia |
| 18 | BS10012: 2017 | British Standard Personal Information Management System |
| 19 |  | 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 Still not in force |
| 20 | FPT Software Personal Data Protection Handbook | PDP\_ Handbook\_Version\_V3.3 |
| 21 | 05e-HD/SG/HDCV/FSOFT | Procedure\_Retention of Records\_V1.2 Guideline\_Personal Data Retention\_v3.3 |

## 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. The Draft PDPD might be finalized and coming in force end of 2022.