Guideline

PERSONAL DATA INVENTORY MANAGEMENT

Document Code	11e-HD/SG/HDCV/FSOFT
Version	3.4
Effective date	01-Aug-2023

TABLE OF CONTENT

RECORD OF CHANGE

No	Effective Date	Version	Change Description	Reason	Reviewer	Final Reviewer	Approver
1	21-Oct-2019	1.0	Newly issued	Legal requirement	MinhPT	Michael Hering	HoanNK
2	11-May-2020	2.1	Update 1. Introduction Add some related document and change related document: "Template_ Inventory_(product)_(dept-function)_(date)" into "Template_Personal Data Processing Inventory"	Update according to Annually revision requirement	TrangNN4	Michael Hering	HoanNK
3	01-Jul-2020	2.1.1	HITRUST	HITRUST requirement	TrangNN4	Michael Hering	HoanNK
4	19-Oct-2020	2.2	Update sections: introduction, purpose, related document, and responsibility	Legal requirement	TrangNN4	Michael Hering	HoanNK
5	01-May-2021	3.0	Change the document structure. Update sections: Introduction, purpose, responsibility	Legal requirement	TrangNN4	Michael Hering	HoanNK
6	01-Oct-2021	3.1	1 added: FPT Software Personal Data Protection Handbook and ISM guidelines, 1.2 added: statement_PIMS scope_V1.0, 3.2 added: statement_PIMS scope_V1.0	Legal requirement	TrangNN4	Michael Hering	HoanNK
7	01-Apr-2022	3.2	2.3 added: Procedure_Retention of Records_V1.1 3.2. 14 added: PDPL, UAR, Decree-Law No. 45 of 2021 3.2. 16 added: Decree of the Vietnamese Government: Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân 3.2. 17 PDP_ Handbook_Version_V 3.2 18: 15e-HD/SG/HDCV/FSOFT	Biannually revision	LinhDTD1	Michael Hering	HoanNK

No	Effective Date	Version	Change Description	Reason	Reviewer	Final Reviewer	Approver
8	01-Nov-2022	3.3	Deleted 2.2: in the DPO tool (WEB application on MS Azure) as the Added 3.3. Data Protection Law, Vietnam, Overview. Added 3.4: Example PII Added 3.2 15 Republic Act 10173 Data privacy Act 2012 Added 4.2 16 Personal Data Protection Act 2010, Malaysia Added 4.2 18 TISAX	Biannually revision	LinhDTD1	Michael Hering	HoanNK
9	01-Aug-2023	3.4	Adjust document version numbers added 3.2 14, 18 changed 3.2 22: Came in force 07/2023 changed 3.3 PDPD was finalized and was coming in force 07/2023	Biannually revision	LinhDTD1	Michael Hering	HoanNK

1 INTRODUCTION

FPT Software Company, Ltd. ("FPT Software" hereinafter) Corporate Data Protection Policy, guidelines, procedures, and templates lay out strict requirements for processing personal data pertaining to customers, business partners, employees or any other individual. It meets the requirements of the European Data Protection Regulation/Directive as well as other national Data Protection Regulations and ensures compliance with the principles of national and international data protection laws in force all over the world. The policies, guidelines, procedures 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.

EU's General Data Protection Regulation and other national/international laws/regulation requires to record all processing activities, which accounts for the ways the data controller and data processor handle the processing of personal data, as well as why those materials are processed.

The personal data inventory gives an overview of FPT Software's data processes under the headings of the GDPR and other national/international laws/regulation.

A data process is everything FPT Software is doing with data. For example:

- Lead data entering the business via an online form
- Upsell campaigns to existing customers via email
- Business development utilizing LinkedIn
- Network building at events (receiving business cards)

Other processes in the business include:

- Handling of employee data for payroll
- Procurement processes and handling of supplier data
- New hire interview / CV processes
- Skill profile database / project staffing

A data process inventory allows FPT Software to list each process individually in order to examine it for GDPR compliance and other national/international laws/regulation.

1.1 Purpose

This guideline sets out an inventory of all type(s) of personal data processed by FPT Software for specific purpose(s) and the period(s) to be compliant with GDPR, article 30 and other national/international personal data protection acts.

For further information on other aspects of data protection and compliance with the GDPR and other personal data protection acts, please refer to FPT Software Corporate Personal Data Protection Policy and the PDP Handbook V3.4.

1.2 Application Scope

See Policy_PIMS scope_V1.3.

1.3 Application of national Laws

The Data Protection Policy, guidelines and templates comprises the internationally accepted data privacy principles without replacing the existing national laws. It supplements the national data privacy laws. The relevant national law will take precedence in the event that it conflicts with the Data Protection Policy and guidelines, or it has stricter requirements than this Policy and guidelines. The content of the Data Protection Policy and guidelines must also be observed in the absence of corresponding national legislation. The reporting requirements for data processing under national laws must be observed.

Each subsidiary or legal entity of FPT Software is responsible for compliance with the Data Protection Policy, this guideline and the legal obligations. If there is reason to believe that legal obligations contradict the duties under the Data Protection Policy or the guidelines, the relevant subsidiary or legal entity must inform the Global Data Protection Officer. In the event of conflicts between national legislation, the Data Protection Policy and this guideline, FPT Software Global Data Protection Officer will work with the relevant subsidiary or legal entity of FPT Software to find a practical solution that meets the purpose of the Data Protection Policy and this guideline.

1.4 Responsibility

The Global Data Protection Officer, appointed by the FPT Software Board Member responsible for Data Protection on behalf of the CEO of FPT Software is fully responsible.

The Global Data Protection Officer (GDPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR) and other national/international laws/regulation.

The GDPO is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements and other Personal Data Protection Acts.

The primary role of the GDPO is to ensure that organization processes, the personal data of employees, customers, providers, or any other individuals in compliance with the applicable data protection rules. GDPO should be able to perform the duties independently.

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

GDPO is responsible to manage and control the personal data inventory.

Risk Management Group

Consultation of departments/units regarding the inventory

Data Protection Representative

Responsible for compiling the contents of the personal data inventory in their department, unit, legal entity, or subsidiary of FPT Software.

More details in Guideline_Personal Data Protection Organization_V3.4.

.

2 GUIDELINE CONTENT

2.1 Records of Processing Activities, GDPR, Article 30

Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all following information:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative, and the data protection officer
- the purposes of the processing
- a description of the categories of data subjects and of the categories of personal data
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations
- where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards
- where possible, the envisaged time limits for erasure of the different categories of data
- where possible, a general description of the technical and organizational security measures referred to in Article 32(1).

Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer

the categories of processing carried out on behalf of each controller

where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards

where possible, a general description of the technical and organizational security measures referred to in Article 32(1).

The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

2.2 Personal data Inventory Execution

Every year every FPT Software department, unit, legal entity, or subsidiary is obligated to perform a personal data inventory managed by GDPO.

After every change of the organizational structure or business process of a department, unit, legal entity or subsidiary, the department, unit, legal entity, or subsidiary is obligated to perform a personal data inventory.

In case of a personal data inventory, the department, unit, legal entity, or subsidiary must use, and fill the "Template_Personal Data Processing Inventory_V2.6" for summary and review of personal data inventory operations. The GDPO is responsible for the input and keeping data Up to Date in the main register of data processing activities.

The execution and completion of personal data inventory is the responsibility of the department Data Protection Representative based on the advice and managed the GDPO. The personal data inventory must be reviewed by the head of relevant department unit, legal entity or subsidiary and then approved by the GDPO.

The Data Protection Representative must hand over the filled "Template_Personal Data Processing Inventory_V2.6" to the risk management group and to the GDPO.

After the assessment of risk management group is completed, the GDPO must review it. GDPO must develop a final privacy impact analysis and risk mitigation plan. The GDPO must bring the results and the mitigation plan to the attention of the FPT Software Board Member responsible for data protection.

2.3 Data Retention

The records of the personal data inventory, the results of the risk assessment shall be kept in accordance with the Guideline_Personal Data Retention_V3.4, Procedure_Retention of Records_V1.3 and the Guideline_Personal Data Protection Policy Development_v2.4.

3 APPENDIXES

3.1 Definition

Abbreviations	Description
PII, Personal Identifiable Information, Personal Data	Refer to the personal data defined by the EU GDPR (Article 4 (1)), 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Subject	EU GDPR (Article 4 - 1), Data subject refers to any individual person who can be identified, directly or indirectly.
Data Controller	EU GDPR (Article 4 - 7), Data Controller means the natural or legal person, public authority, agency or anybody which alone or jointly with others, determines the purpose and means of processing of personal data; where the purpose and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Data Processor	EU GDPR (Article 4 - 8), Data Processor means a natural or legal person, public authority, agency or anybody which processes data on behalf of the controller.
Recipient	EU GDPR (Article 4 - 9), A natural or legal person, public authority, agency or anybody, to which the personal data are disclosed, whether third party or not.
Third Party	EU GDPR (Article 4 - 10), A natural or legal person, public authority, agency or anybody other than the data subject, controller, processor and persons who under direct authority of controller or processor, are authorized to process personal data
DPO/GDPO	Data Protection Officer/Global Data Protection Officer
DPIA	Data Protection Impacted Assessment
PIMS	Personal Information Management System
EU	European Union

3.2 Related Documents

No	Code	Name of documents
1	EU GDPR	EU General Data Protection Regulation
2	95/46/EC	EU Data Protection Directive 95/46/EC
3	Privacy shield	EU-U.S. and Swiss-U.S. Privacy Shield Frameworks designed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.
4	APPI	Act on the Protection of Personal Information, Japan. It came into force on 30 May 2017.
5	PDPA	Personal Data Protection Act 2012, Singapore
6	PDPO	Personal Data (Privacy) Ordinance, Hongkong, 2012
7	PIPA	South Korea's substantial Personal Information Protection Act (PIPA) was enacted on Sept. 30, 2011
8	PIPEDA	Personal Information Protection and Electronic Documents Act, Canada 2018
9	Privacy Act, APPs, CDR	Privacy act Australia including Australian Privacy Principles, Consumer Data Right
10	HITRUST	Health Information Trust Alliance (CSF, Common Security Framework)
11	HIPAA	Health Insurance Portability and Accountability Act of 1996 (HIPAA), US
12	PCI DSS	Payment Card Industry Data Security Standard, May 2018
13	CCPA	California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq.
14	VCDPA	Virginia Consumer Data Protection Act, 01/2023
15	PDPL, UAE	Decree-Law No. 45 of 2021
16	DPA Philippines	Republic Act 10173, Data privacy Act 2012
17	PIPL	Personal Information Protection Law of the People's Republic of China and related laws and regulations

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

3.3 Data Protection Law, Vietnam, Overview

There is no single data protection law in Vietnam. Regulations on data protection and privacy can be found in various legal instruments. The right of privacy and right of reputation, dignity and honour and fundamental principles of such rights are currently provided for in Constitution 2013 ("**Constitution**") and Civil Code 2015 ("**Civil Code**") as inviolable and protected by law.

Regarding personal data, the guiding principles on collection, storage, use, process, disclosure or transfer of personal information are specified in the following main laws and documents:

- **Criminal Code** No. 100/2015/QH13, passed by the National Assembly on 27 November 2015
- Law No. 24/2018/QH14 on Cybersecurity, passed by the National Assembly on 12 June 2018 ("**Cybersecurity Law**");
- Law No. 86/2015/QH13 on Network Information Security, passed by the National Assembly on 19 November 2015; as amended by Law No. 35/2018/QH14 dated 20 November 2018, on amendments to some articles concerning planning of 37 Laws ("**Network Information Security Law**");
- Law No. 59/2010/QH12 on Protection of Consumers' Rights, passed by the National Assembly on 17 November 2010; as amended by Law No.35/2018/QH14 dated 20 November 2018, on amendments to some articles concerning planning of 37 Laws ("**CRPL**");
- Law No. 67/2006/QH11 on Information Technology, passed by the National Assembly on 29 June 2006; as amended by Law No. 21/2017/QH14 dated 14 November 2017 on planning ("**IT Law**");
- Law No. 51/2005/QH11 on E-transactions, passed by the National Assembly on 29 November 2005 ("**E-transactions Law**");
- Decree No. 85/2016/ND-CP dated 1 July 2016, on the security of information systems by classification ("**Decree 85**");
- Decree No. 72/2013/ND-CP dated 15 July 2013 of the Government, on management, provision and use of Internet services and online information; as amended by Decree No. 27/2018/ND-CP dated 1 March 2018 and Decree No.150/2018/ND-CP dated 7 November 2018 ("**Decree 72**");
- Decree No. 52/2013/ND-CP dated 16 May 2013 of the Government; as amended by Decree No. 08/2018/ND-CP dated 15 January 2018, on amendments to certain Decrees related to business conditions under state management of the Ministry of Industry and Trade and Decree No. 85/2021/ND-CP dated 25 September 2021 ("**Decree 52**");
- Decree No. 15/2020/ND-CP of the Government dated 3 February 2020 on penalties for administrative violations against regulations on postal services, telecommunications, radio frequencies, information technology and electronic transactions ("**Decree 15**");
- Circular No. 03/2017/TT-BTTTT of the Ministry of Information and Communications dated 24 April 2017 on guidelines for Decree 85 ("**Circular 03**");

- Circular No. 20/2017/TT-BTTTT dated 12 September 2017 of the Ministry of Information and Communications, providing for Regulations on coordinating and responding to information security incidents nationwide ("**Circular 20**");
- Circular No. 38/2016/TT-BTTTT dated 26 December 2016 of the Ministry of Information and Communications, detailing cross-border provision of public information ("**Circular 38**");
- Circular No. 24/2015/TT-BTTTT dated 18 August 2015 of the Ministry of Information and Communications, providing for the management and use of Internet resources, as amended by Circular No. 06/2019/TT-BTTTT dated 19 July 2019 ("**Circular 25**"); and
- Decision No. 05/2017/QD-TTg of the Prime Minister dated 16 March 2017 on emergency response plans to ensure national cyber-information security ("**Decision 05**").

Applicability of the legal documents will depend on the factual context of each case, e.g businesses in the banking and finance, education, healthcare sectors may be subject to specialized data protection regulations, not to mention to regulations on employees' personal information as provided in Labour Code 2019 ("**Labour Code**").

The most important Vietnamese legal documents regulating data protection are the Cybersecurity Law and Network Information Security Law. Cybersecurity laws in other jurisdictions that were inspired by the GDPR of the EU, the Cybersecurity Law of Vietnam shares similarities with China's Cybersecurity Law enacted in 2017. The law focuses on providing the government with the ability to control the flow of information. The Network Information Security Law enforces data privacy rights for individual data subjects.

A draft Decree detailing a number of articles of the Cybersecurity Law ("**Draft Cybersecurity Decree**"), notably including implementation guidelines for data localization requirements, together with a draft Decree detailing the order of and procedures for application of a number of cybersecurity assurance measures and a draft Decision of the Prime Minister promulgating a List of information systems important for national security, are being prepared by the Ministry of Public Security ("**MPS**") in coordination with other relevant ministries, ministerial-level agencies and bodies.

MPS has drafted a Decree on personal data protection ("**Draft PDPD**"), which is contemplated to consolidate all data protection laws and regulations into one comprehensive data protection law as well as make significant additions and improvements to the existing regulations. The Draft PDPD was released for public comments in February 2021 and was originally scheduled to take effect by December 2021. The Finalization process consuming much more time than the MPS first anticipated. PDPD was finalized and was coming in force 07/2023.

3.4 Example PII: