Template

DPO JOB DESCRIPTION

Document Code	36e-BM/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 7.2, 8.2.1.1, 8.2.1.2, 8.2.1.3, 8.2.1.4, 8.2.5	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 4.2 13 added PIPL, 4.2 14 added: PDPL, UAR, Decree-Law No. 45 of 2021 4.2 16 added: Decree of the Vietnamese Government: Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân 4.2 17 PDP_ Handbook_Version_V3.2 4.2 18: 15e-HD/SG/HDCV/FSOFT	Linh Do Thi Dieu	Michael Hering	CFO/COO
3	01-Nov-2022	1.2	Biannually revision	Added 4.3. Data Protection Law, Vietnam, Overview. Added 4.2 15 Republic Act 10173 Data privacy Act 2012 Added 4.2 17 PDPA Added 4.2 18 TISAX	Linh Do Thi Dieu	Michael Hering	CFO/COO
4	01-Aug-2023	1.3	Biannually revision	Adjust document version numbers Added 2 Article 28 of PDPD 13 Vietnam added 4.2 14, 18 changed 4.2 22: Came in force 07/2023 changed 4.3 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, 1.3 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, PDPD13 VN 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_v3.5 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 purpose it to drive compliance with the EU General Data Protection Regulation (GDPR), PDPD13 and other national/international Data Protection Regulations and ensure ongoing compliance of all core activities for FPT Software.

1.2 Application Scope

In scope are 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. See Policy_PIMS Scope_v1.4.

1.3 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), APPI, PDPA, PIPA, PDPD13 and other national laws. 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.

The Data Protection Officer reports directly to the board member responsible for data protection CFO.

Note that Article 24(1) states that data protection compliance is a corporate responsibility of the data controller, not of the Data Protection Officer.

The GDPO is the owner of this document and is responsible for ensuring that this template is reviewed in line with the review requirements of the EU GDPR.

2 Responsibilities

The Data Protection Officer will maintain expert knowledge of data protection law and practices, as well as other professional qualities, to ensure that FPT Software complies with the requirements of the EU GDPR and other relevant data protection law(s) and regulations.

Reporting directly to the board member responsible for data protection (compliance), the Data Protection Officer must inform and advise on the protection of personal data in relation to the EU GDPR and other relevant data protection law(s) and regulations.

The Data Protection Officer will ensure that documentation to demonstrate compliance with the GDPR such as policies, guidelines, procedures, and templates are kept up to date. For example, the register of processing required under Article 30. Furthermore, the Data Protection Officer will plan and schedule data processing audits regularly, monitoring core activities to ensure they comply with the EU GDPR and.

The Data Protection Officer is the main contact point for employees and will liaise with all members of staff on matters of data protection.

Key tasks of the Data Protection Officer (Article 39, (1) and Recital 97):

Inform and advise all members of staff on their obligation to adhere to the EU GDPR and law(s) when dealing with personal data (Article 39(1)(a)).
Monitor compliance with the EU GDPR and other relevant data protection law(s) and regulations
Advise and inform on the data protection impact assessment (DPIA), including monitoring performance of DPIAs against the requirements of the EU GDPR Article 35 (Article 39(1)(c)).
Liaise and cooperate with the supervisory authority (Article 39(1)(d)).
Be point of contact for the supervisory authority on issues relating to processing of personal data, and to consult with the supervisory authority, where necessary, on any other personal data matters (Article 39(1)(e)).
Contribute to the development and maintenance of all FPT Software data protection policies, procedures, and processes in relation to the protection of personal data.
Advise management on the allocation of responsibilities internally to support ongoing compliance with the EU GDPR and other relevant data protection law(s) and regulations.
Ensure training and awareness is available and delivered to all members of staff involved in processing operations relating to personal data.
Regularly monitor compliance with the EU GDPR and other relevant data protection law(s) and regulations by conducting audits of processes relating to personal data, and report to the Board of Directors.
Be point of contact for data subjects regarding the processing of their personal data.
Be point of contact for customer and 3rd party providers regarding the processing of personal data.
Monitor compliance with the Data Protection Policy (Policy_Personal Data Protection Management_v3.5) throughout FPT Software and to develop/advise on procedures for effective security.

Advise senior management on the allocation of information security responsibilities.

Develop/advise on formal procedures for reporting incidents (EU GDPR and information security-related) and investigations under Articles 33 and 34 of the GDPR.

Contribute to the business continuity and disaster recovery planning process.

Advise on and monitor the safeguarding of organizational record management, (Retention of Records Procedure (Procedure_Retention of Records_V1.4, Guideline_Personal Data Retention_v3.5)

Work with information asset owners to ascertain the extent to which personal data is collected, held and/or used in FPT Software, and that it is properly controlled and safeguarded from loss of confidentiality, integrity, or availability from any cause (WP29 states 'DPOs often create inventories and hold a register of processing operations based on information provided to them by the various departments in their organization responsible for the processing of personal data. This practice has been established under many current national laws and under the data protection rules applicable to the EU institutions and bodies').

Ensure that records of the processing are kept by FPT Software as detailed in Article 30 mentioned above.

Advise the controller of its obligation to issue privacy notices to data subjects at the point of collection of their personal data under Articles 13 to 15.

With the benefit of time to explore the field of data protection, and to consider potential areas of activity, the following items should be added.:

Review and appraise the soundness, adequacy and application of security and other controls for the protection of data.

Identify and test the controls and, where appropriate, to suggest additional controls, which may be established to maintain the confidentiality, integrity, and availability of personal data.

Bring to the attention of Board of Directors (Top level management) as appropriate any matters which are potential risk factors to the proper safeguarding of personal data within FPT Software.

The Data Protection Officer is authorized to have access to all FPT System's systems relating to the collection, processing, and storage of personal data for the purpose of assessing the use and security of personal data. The Data Protection Officer may expect the cooperation of all staff in carrying out these duties, including access to systems and records. If cooperation is not being forthcoming, the Data Protection Officer will report to the Board of Directors (Top level management) accordingly.

Article 28 of PDPD 13 Vietnam requires a data controller and/or a data processor to appoint a department to protect personal data and to appoint a data protection officer (DPO) if there is sensitive personal data involved. The information of such DPO must be notified to the Cybersecurity Department.

3 Document Owner and Approval

The Head of HR (CHRO) in collaboration with the Global Data Protection Officer 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_Personal Data Protection Policy Development_V2.5.

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

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

4. APPENDIXES

4.1 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

4.2 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

4.3 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 honor 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.