

***Template***

**Internal Audit Report**

|  |  |
| --- | --- |
| Document Code | 43e-BM/SG/HDCV/FSOFT |
| Version | 1.1 |
| Effective date | 01/11/2022 |

Table of content

[1 INTRODUCTION 4](#_Toc118731482)

[1.1 Purpose 4](#_Toc118731483)

[1.2 Application Scope 4](#_Toc118731484)

[1.3 Responsibility 5](#_Toc118731485)

[2 TEMPLATE/ FORM 6](#_Toc118731486)

[3. APPENDIXES 8](#_Toc118731487)

[3.1 Definition 8](#_Toc118731488)

[3.2 Related Documents 9](#_Toc118731489)

[3.3 Data Protection Law, Vietnam, Overview 11](#_Toc118731490)

RECORD OF CHANGE

| No | Effective Date | Version | Change Description | Reason | Reviewer | Final Reviewer | Approver |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 01.04.2022 | 1.0 | Newly issued | BS 10012:2017 Requirements/GDPR, clause 9.2 | LinhDTD1 | Michael Hering | HoanNK |
| 2 | 01.11.2022 | 1.1 | Added 3.3. Data Protection Law, Vietnam, Overview.  Added 3.2 15 Republic Act 10173  Data privacy Act 2012  Added 3.2 17 PDPA  Added 3.2 18 TISAX | Biannually revision | LinhDTD1 | Michael Hering | HoanNK |

# 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.

## Purpose

This template should support the GDPO and/or the auditor by document the audit results.

## Application Scope

See statement\_PIMS scope\_V1.2.

## 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 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.

GDPO must ensure that all departments of the company are following the company guidelines and the respective laws.

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.

This template was approved by the GDPO on 01.11.2022 and is issued on a version-controlled basis under his signature

Signature: Date: 01.11.2022



# TEMPLATE/ FORM

|  |  |
| --- | --- |
| **INTERNAL AUDIT REPORT GPDO SHEET** | **Document Control**  Document Code:  Issue No:  Issue Date: |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Scope & Type of Audit (incl. Site, Unit, legal entity): | | | | Report No. | |
| Date: | |
|  | | | | Auditors: | |
| PDP Compliance: | | | |  | |
| Persons Contacted: | |  | | Previous Audit  Ref. No. | |
| GDPO: | |  | | BU Head/FSU Lead  Signature: | |
| Management System Documentation/Aspects Covered: | |  | |  | |
| Summary of Audit: | | No. of Non-conformities: |  | No. of Observations: |  |
|  | | | | | |
| GDPO Signature: | | | | Date: | |
| Incident/Improvement Action Reports Raised: (Ticked box = completed) | | | | | |
| 1. | 🞏 | 2. | 🞏 | 3. | 🞏 |
| 4. | 🞏 | 5. | 🞏 | 6. | 🞏 |
| 7. | 🞏 | 8. | 🞏 | 9. | 🞏 |
| 10. | 🞏 | 11. | 🞏 | 12. | 🞏 |
| BU Lead/FSU Head Signature (Actions Completed): | | | | Date: | |

# 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 | 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 | TISAX | Trusted information security assessment exchange |
| 19 | BS10012: 2017 | British Standard Personal Information Management System |
| 20 |  | 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 |
| 21 | FPT Software Personal Data Protection Handbook | PDP\_ Handbook\_Version\_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 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. The Draft PDPD might be finalized and coming in force end of 2022.