Procedure

MANAGEMENT OF SUB-CONTRACTED PROCESSING

Document Code	21e-QT/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 ADPO	Final Reviewer GDPO	Approver Board member
1	01-Jul-2021	1.0	Newly issued	BS 10012:2017 Requirements/GDPR, Clause 8.2.7.4. 8.2.11.9	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 16 PIPL 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 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	ISO27701 requirements	Update version Added PDPD13 Added 1.4 sentence: The Global Data Protection Officer is… Added 1.4 paragraph: Relationship owner supported by… Added 1.5 Added 2 paragraph: Requirements regarding sub-contract:.. Added 3 fptsoftware.com Added 4.2 18 Changed 4.2 & 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 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 Data Protection Policy provides one of the necessary framework conditions 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, PDPD13 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.

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

All external suppliers (processor, sub-processor) that process personal data on behalf of FPT Software are within the scope of this procedure.

All processing of personal data by FPT Software is within the scope of this procedure.

Means, 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.

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_v1.4.

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 is responsible for approving the selection of all sub-contracted processors of personal data in line with the requirements of this procedure.

The owners of third-party relationships (FSU, OB) are responsible for ensuring that all external data processing is contracted out in line with this procedure.

The Head of IT is responsible for ensuring that adequate technical and other resources that might be required are made available to support the relationship owner in the monitoring and management of the relationship.

The Global Data Protection Officer is responsible together with the relationship owner to determine and maintain active communication with third parties.

Relationship owner supported by GDPO is responsible to inform third parties without any undue delay about any changes about the obligations to data subjects including modification or withdrawal of consent, requests for correction, erasure, or restrictions on processing, or objections to the processing of personal data requested by the data subject. The relationship owner must monitor the acknowledgement of receipt of this information.

The Global Data Protection Officer is responsible for carrying out regular audits of third-party compliance.

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

1.5 Sub-processor role and Definition

A sub-processor is an entity engaged by a data processor to assist in fulfilling the processing of personal data. Contrary to a processor, which is directly involved in the processing for the controller, a sub-processor works under the instruction of the processor, carrying out specific tasks that involve personal data.

The main distinction between a sub-processor and a processor lies in their relational hierarchy and scope of authority. The processor is an independent entity that determines how to process personal data on behalf of the controller. A sub-processor does not have this level of autonomy and operates under the processor's directives. Responsibilities of a sub-processor include storage, analysis, or other data handling tasks as assigned by the processor.

While a subprocessor and a processor perform similar functions in terms of data handling, their relationship with the controller differs significantly. The controller determines the "what" and "why" behind personal data processing and is ultimately responsible for its protection and compliance with data protection laws. The sub-processor acts on behalf of the processor and does not have direct control over the processing purposes or means, positioning them further down the operational hierarchy.

Entities within the data processing hierarchy must uphold data protection and privacy standards. Understanding these roles is crucial for compliance and effective data management.

The compliance landscape for sub-processors hinges on stringent legal requirements, GDPR, PDPD13 and other national/international laws. These entities must adhere to a clear legal framework, which includes obligations and the necessity to establish a data processing agreement (DPA).

The law stipulates that a legal binding agreement must be in place between the data processor and a sub-processor. This contractual linkage ensures a chain of accountability in the protection of personal data.

When engaging a sub-processor, it is essential to ensure they can uphold the necessary standards of data protection and follow prescribed instructions precisely. Due diligence in selection and clarity in defining responsibilities is critical to maintaining compliance with data protection laws.

The selection of a data subprocessor requires a rigorous assessment of their capabilities to handle data securely and fulfill the obligations set by the data processor and controller. Criteria for selection include:

- Compliance: The subprocessor must demonstrate compliance with relevant data protection legislation, such as the GDPR, PDPD13 or other national/international laws.
- Security Measures: They must have robust security measures in place to safeguard personal data from unauthorized access, disclosure, or alteration.
- Experience and Reliability: Their track record in managing sensitive data should be scrutinized to ensure reliability.

A data sub-processor is bound by stringent security and confidentiality obligations to protect the integrity of the data. They must:

- Maintain an adequate level of protection that aligns with or exceeds the standards of the data processor.
- Implement and regularly review technical and organizational measures to prevent data breaches.

2 Procedure

FPT Software selects only suppliers that can provide technical, physical and organizational security that meet FPT Software's requirements in terms of all the personal data they will process on FPT Software's behalf.

The Procurement Department in collaboration with LCM and the Global Data Protection Officer has in place appropriate checks that ensure all contracts are reviewed to see if personal data is processed. These checks are carried out even if data processing activities are not the primary reason for the contract.

The data controller (FPT Software) will ensure that all security arrangements are outlined in the contract with the external processor.

Suppliers from outside the EU will only be selected under the following conditions, in addition to the conditions noted elsewhere in this procedure:

- If the supplier or the state in which it resides has been positively identified in an adequacy decision by the EU Commission; or
- Where there are legally binding corporate rules or a standard contract clause, and organizational and technical safeguards, established between FPT Software and the supplier to secure the rights and freedoms of data subjects at least equal to those afforded within the EU; or
- Where the arrangement has been approved by the supervisory authority.

An information security risk assessment or data protection impact assessment, considering the information security controls of ISO 27001 Annex A, is carried out before a supplier is engaged. Supplier risk assessments are conducted in line with Procedure_Data Protection Impact Assessment_v1.4 and Guideline_Risk Management_DPIA_v2.5.

If the Global Data Protection Officer considers it necessary because of the nature of the personal data to be processed or because of the circumstances of the processing, an audit of the supplier's security arrangements against the requirements of ISO 27001 may be conducted before entering into the contract. Supplier audits are conducted in line with Managing Third Party Service Contracts (Procedure_Third Party Service Contracts Management_v1.4).

FPT Software requires a written agreement to provide the service as specified and requires the supplier to provide appropriate security for the personal data it will process.

All data processing contracts allow FPT Software to conduct regular audits of the supplier's security arrangements during the period in which the supplier has access to the personal data.

All data processing contracts forbid suppliers from using further subcontractors without FPT Software's written authorization for the processing of personal data.

Where FPT Software permits a supplier to subcontract processing of personal data, the immediate supplier must prohibit the second-level contractor (or further down the chain) from subcontracting these processing operations without FPT Software's written authorization.

Contracts with second-level subcontractors will only be approved if they require the subcontractors to comply with at least the same security and other provisions as the primary subcontracting organization (the supplier) if they specify that, when the contract is terminated, related personal data will either be destroyed or returned to FPT Software, and so on down the chain of sub-contracting.

FPT Software must determine and maintain active communication with third parties. Relationship owner supported by GDPO will inform third parties without any undue delay about any changes about the obligations to data subjects including modification or withdrawal of consent, requests for correction, erasure, or restrictions on processing, or objections to the processing of personal data requested by the data subject. The relationship owner must monitor the acknowledgement of receipt of this information. GDPO will review it in the data inventory session and during internal audit (Guideline_Personal Data Inventory Management_v3.5, Guideline_Personal Data Protection Management Audit_v2.5).

Requirements regarding sub-contract:

The sub-contract (or other legal act) must setsout details of the processing including:

☐ the subject matter of the processing;

☐ the duration of the processing;

☐ the nature and purpose of the processing;

☐ the type of personal data involved;

☐ the categories of data subject;

☐ the controller's obligations and rights.

The sub-contract or other legal act must include terms or clauses stating that:

☐ the processor must only act on the controller's documented instructions, unless required by law to act without such instructions;

☐ the processor must ensure that people processing the data are subject to a duty of confidence;

☐ the processor must take appropriate measures to ensure the security of processing;

☐ the processor must only engage a sub-processor with the controller's prior authorisation and under a written contract;

☐ the processor must take appropriate measures to help the controller respond to requests from individuals to exercise their rights;

☐ taking into account the nature of processing and the information available, the processor must assist the controller in meeting its legal obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;

☐ the processor must delete or return all personal data to the controller (at the controller's choice) at the end of the contract, and the processor must also delete existing personal data unless the law requires its storage; and

☐ the processor must submit to audits and inspections. The processor must also give the controller whatever information it needs to ensure they are both meeting their legal obligations.

Depending on the country and the regional coverage (data transfer) Template_Personal Data Protection Exhibit_v1.7 or Template_Data Processing Agreement_v1.5 should be used. GDPO must be involved by Contract Management System.

3 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_Personal Data Protection Policy Development_v2.5.

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

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

4 APPENDIX

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/ADPO	Data Protection Officer/Global Data Protection Officer/Assistant 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	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 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	PDPD13, VN	Decree of the Vietnamese Government: PDPD13 Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân 07/2023
24	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 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.