Procedure

PERSONAL DATA BREACH NOTIFICATION

Document Code	20e-QT/SG/HDCV/FSOFT
Version	1.3.1
Effective date	14-May-2024

TABLE OF CONTENT

RECORD OF CHANGE

No	Effective Date	Version	Reason	Change Description	Reviewer	Final Reviewer	Approver
1	01-Jul-2021	1.0	Newly issued	BS 10012:2017 Requirements/GDPR, Clause 8.2.11.7	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 1.4 changed: Policy_Personal Data Protection Training_v1.1 2.0 changed: template_DS request_incident_compliant_appeal_register-DP_V1.2 6.2 13 added PIPL, 6.2 14 added: PDPL, UAR, Decree-Law No. 45 of 2021 6.2 16 added: Decree of the Vietnamese Government: Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân 6.2 17 PDP_ Handbook_Version_V3.2 6.2 18: 15e-HD/SG/HDCV/FSOFT	Linh Do Thi Dieu	Michael Hering	CFO/COO
3	01-Nov-2022	1.2	Biannually revision	Added 6.3. Data Protection Law, Vietnam, Overview. Added 3.2 15 Republic Act 10173 Data privacy Act 2012 Added 6.2 16 PIPL Added 6.2 17 PDPA Added 6.2 18 TISAX	Linh Do Thi Dieu	Michael Hering	CFO/COO
4	01-Aug-2023	1.3	Biannually revision	Adjust document version numbers added 6.2 14, 18 changed 6.2 22: Came in force 07/2023 changed 6.3 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

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 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_v3.4.1 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 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 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.

This procedure applies in the event of a personal data breach under Article 33 of the GDPR – *Notification of a personal data breach to the supervisory authority* – and Article 34 – *Communication of a personal data breach to the data subject*.

The GDPR draws a distinction between a 'data controller' and a 'data processor' to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Each organisation should establish whether it is data controller, or a data processor for the same data processing activity; or whether it is a joint controller. See Policy_PIMS Scope_v1.3.1.

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 procedure, FPT Software GDPO 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 performing necessary checks on personal data to establish the need for conducting a DPIA.

All users (whether Employees/Staff, contractors or temporary Employees/Staff and third-party users) *of* FPT Software are required to be aware of, and to follow this procedure in the event of a personal data breach (reference Policy_Personal Data Protection Training_v1.4.1).

All Employees/Staff, contractors or temporary personnel are responsible for reporting any personal data breach to the Global Data Protection Officer.

The Data Protection Officer (DPO) has a specific task under article 39 of the GDPR to coordinate with the supervisory authority and act as the focal point for matters pertaining to processing.

The Global Data Protection Officer is responsible for the application and effective working of this procedure, and for reporting to the information owner (HRPR, COO, CFO …).

2 Procedure, Breach Notification Data Processor to Data Controller

FPT Software reports any personal data breach or security incident to the data controller without undue delay. The contact details are recorded in the Internal Breach Register (Template_DS Request_Incident_Compliant_Appeal_Register-DP_V1.4.1).

FPT Software provides the controller with all the details of the breach.

The breach notification is made by email and telephone call.

A confirmation of receipt of this information is made by email.

3 Procedure, Breach Notification Data Controller to Supervisory Authorities

FPT Software determines if the supervisory authority need to be notified in the event of a breach.

FPT Software assesses whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach, by conducting DPIA (Template_DPIA_compact_V1.3.1, Template_Risk Management DPIA_v3.4.1) against breach.

If a risk to data subject(s) is likely, FPT Software reports the personal data breach to the supervisory authority without undue delay, and not later than 72 hours.

If the data breach notification to the supervisory authority is not made within 72 hours, FPT Software's Global Data Protection Officer submits it electronically with a justification for the delay.

If it is not possible to provide all necessary information at the same time FPT Software will provide the information in phases without undue further delay.

The following information needs to be provided to the supervisory authority (Template_DS Request_Incident_Compliant_Appeal_Register-DP_V1.4.1):

A description of the nature of the breach

The categories of personal data affected

Approximate number of data subjects affected

Approximate number of personal data records affected

Name and contact details of the Global Data Protection Officer

Consequences of the breach (This should include consequences both those that have already occurred and those that are likely to occur)

Any measures taken to address the breach

Any information relating to the data breach

The Global Data Protection Officer notifies the respective supervisory authority. Contact details for the supervisory authority are recorded in the Schedule of authorities and key suppliers (Record_Schedule_ Authorities_Key Suppliers_V1.3.1).

In the event the supervisory authority assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register Template_DS request_incident_compliant_appeal_ register - DP_V1.4.1.

The breach notification is made by email, phone call.

A confirmation of receipt of this information is made by email, phone call.

4 Procedure, Breach Notification Data Controller to Data Subject

If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, FPT Software notifies the data subjects affected immediately by Global Data Protection Officer.

The notification to the data subject describes the breach in clear and plain language, in addition to information specified above.

FPT Software takes measures to render the personal data unusable to any person who is not authorised to access it using encryption.

The data controller takes subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur.

If the breach affects a high volume of data subjects and personal data records, FPT Software decides based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder the FPT Software's ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication (Procedure_Communication_V1.3) or similar measure informs those affected in an equally effective manner.

If FPT Software has not notified the data subject(s), and the supervisory authority considers the likelihood of a data breach will result in high risk, FPT Software will communicate the data breach to the data subject by email.

FPT Software documents any personal data breach(es), incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.

5 Document Owner and Approval

The 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_Policy_Development_V2.4.1.

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

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

6 APPENDIX

6.1 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

6.2 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_V3.4.1

6.3 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.