Policy

FPT Software Corporate Data Protection Policy

PERSONAL DATA PROTECTION MANAGEMENT

Document Code	03e-QD/SG/HDCV/FSOFT
Version	3.4.1
Effective date	14-May-2024

TABLE OF CONTENT

RECORD OF CHANGE

No	Effective Date	Version	Change Description	Reason	Reviewer	Final Reviewer	Approver
1	10-May-2019	1.0	Newly issued	Business requirement	Trang	Michael Hering	CFO/COO
2	21-Oct-2019	1.1	Add content of Introduction section -Adjust the purpose -Adjust the application scope -Add application of national Laws -Add some new definitions -Update related documents -Update content of guiding principles -Add new section "Customer and Provider Data (3rd party)", "Employee data", "Data Protection Control", "Global Data Protection Officer" -Change section "Disciplinary" to "Responsibilities and Disciplinary", update content -Update content of sections: Announce and Release, Exception	Legal requirement	Trang	Michael Hering	CFO/COO
4	11-May-2020	2.1	-Add sections and sub-sections:4 PERSONAL DATA PROTECTION TRAINING7 SUPPLEMENTARY GUIDELINES AND DOCUMENTS -Add some related document at Related Document Section	Update according to Annually revision requirement	Trang	Michael Hering	CFO/COO
5	01-Jul-2020	2.1.1	HITRUST	HITRUST requirements	Trang	Michael Hering	CFO/COO
6	19-Oct-2020	2.2	Update sections: related document, 2.4 Policy Review and Evaluation, 4. Personal data protection training, 7. supplementary guidelines and documents	Legal requirement	Trang	Michael Hering	CFO/COO
7	01-May-2021	3.0	Change document structure. Update sections: GLOBAL DATA PROTECTION OFFICER, SUPPLEMENTARY GUIDELINES AND DOCUMENTS and Related Document Add 9. Appendixes.	Legal requirement	Trang	Michael Hering	CFO/COO
8	01-Oct-2021	3.1	Update 1.2 Application scope, 2.4 add: Guideline_Personal Data Protection Policy Development_v2.0, 4 add: Policy_Personal Data Protection Training_v1.1, 5 add: Template_DPO Job Description_v1.0, 7 add: procedures, statements, templates	Legal requirement	Trang	Michael Hering	CFO/COO

No	Effective Date	Version	Change Description	Reason	Reviewer	Final Reviewer	Approver
9	01-Apr-2022	3.2	Update 1.2: Policy_PIMS Scope_v1.1 Update 2.4: Guideline_Personal Data Protection Policy Development_v2.2 Update 4: see Policy_Personal Data Protection Training_v1.2 Update 5: Template_DPO Job Description_v1.1 Update 7: version updates 9.1 14 added; PDPL, UAR 9.1 16 added: Decree of the Vietnamese Government: Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân	Legal requirement	Linh Do Thi Dieu	Michael Hering	CFO/COO
10	01-Nov-2022	3.3	Change 2.2.1, added 4. Technical and Organizational measures. Added 10.3 Data Protection Law, Vietnam, Overview. Added 10.2 15 Republic Act 10173 Data privacy Act 2012 Added 10.2 17 PDPA Added 10.2 18 TISAX	HITURST requirement	Linh Do Thi Dieu	Michael Hering	CFO/COO
11	01-Aug-2023	3.4	Changed email to michael.hering@fpt.com Added 10.2 14, 18 Changed 10.02 22: Came in force 07/2023 Changed 10.3 PDPD was finalized and was coming in force 07/2023. Add 6: Article 28 of PDPD VN	Biannually revision	Linh Do Thi Dieu	Michael Hering	CFO/COO
12	14-May-2024	3.4.1	Added 2.4 Access Request of state/government or federal agency or other regulatory body change document classification, from ‘internal use’ to ‘public’	HITURST requirement	Linh Do Thi Dieu	Michael Hering	CFO/COO

1. INTRODUCTION

FPT Software Company, Ltd. ("FPT Software" hereinafter) Corporate Data Protection Policy lays 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 Directive and ensures compliance with the principles of national and international data protection laws in force all over the world. The policy sets 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.

FPT Software managers and employees are obligated to adhere to the Corporate Data Protection Policy and observe their local data protection laws. As the Global Data Protection Officer, it is my duty to ensure that the rules and principles of data protection at FPT Software are followed around the world.

I will be pleased to answer any questions you have about data protection and international personal data transfer.

Michael Hering
Global Data Protection Officer, michael.hering@fpt.com, +84 902606236

1.1 Purpose

This Data Protection Policy applies worldwide to FPT Software, Subsidiaries as well legal entities and is based on globally accepted, basic principles of 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 an adequate level of data protection prescribed by the European Union General Data Protection Regulation, APPI, PDPA or other national Personal Data Protection Regulations and national laws for cross-border data transmission, including to countries which do not have adequate data protection law, yet.

In order 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 and information security policies.

1.2 Application Scope

See Policy_PIMS Scope_v1.31

1.3 Application of national Laws

This Data Protection Policy 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 this Data Protection Policy, or it has stricter requirements than this Policy. The content of this Data Protection Policy 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 this Data Protection Policy and the legal obligations. If there is reason to believe that legal obligations contradict the duties under this Data Protection Policy, the relevant subsidiary or legal entity must inform the Global Data Protection Officer. In the event of conflicts between national legislation and the Data Protection Policy, FPT Software in person the 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.

1.4 Prevention of national and international Data Protection Laws Violations

The Global Data Protection Officer GDPO reporting to the board member responsible for Data Protection CFO oversees the compliance and regulatory functions FPT Software, with the goal to identify, reduce, and monitor all areas of possible regulatory and reputational risk regarding personal data processing.

The Personal Data Protection Handbook (policies, guidelines, procedures, templates) is revised and supplemented twice a year. The GDPO coordinates any revisions or supplements to the Handbook. The GDPO and final CFO reviews and approves the Handbook promptly in the event of any material change in laws. regulations or business practices.

The Personal Data Protection Handbook (policies, guidelines, procedures, templates) is published on FPT Software’s QMS, all employees have access to QMS. Relevant portions of the Handbook are distributed promptly upon material changes in the Handbook. New employees are informed about the Handbook and QMS. They are required to review the Handbook and certify that they understand the relevant provisions of the Handbook as it applies to that employee.

GDPO provides periodically an online personal data protection education programs on e-campus FPT Software’s online training platform to keep employees informed about current regulatory developments, updates of policies and procedures, and legal requirements. See Policy_Personal Data Protection Training_v3.4.1.

If a violation of the Personal Data Protection Handbook (policies, guidelines, procedures, templates) occurs or a preliminary determination is made that a violation may have occurred, a report must made to the GDPO and Senior Management.

The Senior Management should impose adequate sanctions on employees violating the policies contained in the Handbook. Sanctions may include any or all of the following: a letter of censure, a fine, temporary suspension of employment, termination of employment, or any other sanction deemed appropriate by Senior Management.

2. POLICY

2.1 Guiding principles

Principle 1: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency). Collection, processing, transfer, and use of personal data in an illegal way or non-administrative business operations are strictly prohibited.

Principle 2: Processing of personal data only where this is strictly necessary for legal and regulatory purposes, or for legitimate organizational purposes.

Collection only for specified, explicit and legitimated purpose and not further processed in a manner that is incompatible with those purpose (purpose limitation).

Principle 3: Processing only of the minimum of personal information required for these purposes. Adequate, relevant, and limited to what is necessary in relation to the purpose for which they are processed (data minimization).

FPT Software will only collect, process, transfer, and use the personal data provided by parties within the scope of laws, regulations, and business requirements, and will take appropriate and reasonable measures to handle and use the personal data within the necessary and reasonable scope.

Principle 4: Providing clear information to data subjects (including children) about how their personal information are used and by whom.

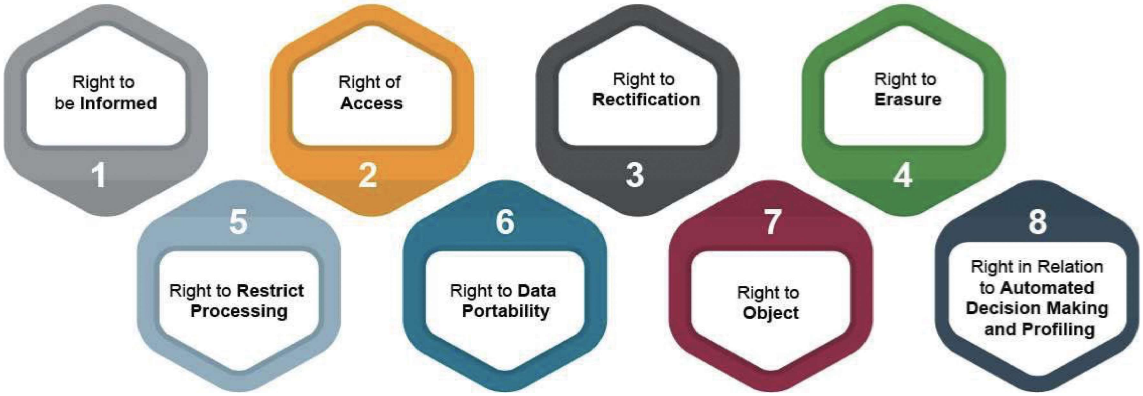
Principle 5: Ensuring special safeguards, if collecting information directly from children.

Principle 6: Only processing relevant and adequate personal information. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purpose for which they are processed, are erased, or rectified without delay (accuracy).

Principle 7: Maintaining a documented inventory of the categories of personal information processed by FPT Software.

Principle 8: Retaining personal information only for as long as is necessary for legal or regulatory reasons or for legitimate organizational purposes and ensuring timely and appropriate disposal (storage limitation).

Principle 9: Respecting data subject right in relation to their personal information.


Right to be Informed
1
Right of Access
2
Right to Rectification
3
Right to Erasure
4
5
Right to Restrict Processing
6
Right to Data Portability
7
Right to Object
8
Right in Relation to Automated Decision Making and Profiling

Principle 10: Processing in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, by using appropriate technical or organizational measures. (Integrity and confidentiality)

Principle 11: GDPR and other national and international laws restricts the transfer of personal data to countries for example outside the EEA or relevant countries. These restrictions apply to all transfers, no matter the size of transfer or how often you carry them out, unless the rights of the individuals in respect of their personal data are protected in another way. Only transferring personal data if it is subject to 'appropriate safeguards', which are listed in the GDPR or other national and international laws.

Principle 12: Used Appropriate safeguards are Standard Data Protection Clauses adopted by the Commission. The clauses contain contractual obligations on the data exporter and the data importer, and rights for the individuals whose personal data is transferred. Individuals can directly enforce those rights against the data importer and the data exporter. SCC must be used in their entirety and without amendment.

Principle 13: Developing and implementing a PIMS to enable the PIMS policy to be implemented.

Principle 14: Identification of people/employees with specific responsibility and accountability for the PIMS. Implementation of a strong governance including a Global Data Protection Officer.

Principle 15: Maintain records of processing of personal information.

FPT Software employees breach these principals are fined based on the labor contract regulations.

2.2 Customer and Provider Data (3rd party)

2.2.1 Data processing for a contractual relationship

Personal data of customers and providers (3rd party) can be processed in order to establish, execute and terminate a contract. Prior to a contract – during the contract initiation phase – personal data can be processed to prepare bids or purchase orders or to fulfill other requests that relate to contract conclusion. Customers or providers can be contacted during the contract preparation process using the information that they have provided. Any restrictions requested by customers or providers must be complied with.

The public, means every customer, provider, data subjects must have access to information about the FPT Software's Personal Data Protection principles and activities (see Chapter 4) and must be able to communicate with FPT Software's Global Data Protection Officer in an easy way:

Michael Hering | Global Data Protection Officer, Director | *FPT SOFTWARE*

F-Town Building 3, Saigon Hi-Tech Park, Lot T2, D1 St., Tan Phu Ward, Thu Duc City, HCM City, Vietnam
Cell: +84 90 2606236 | Tel: +84 (8) 3 736 2323 | Fax: +84 (8) 3 736 3333

URL: www.fpt-software.com

The Policy Personal Data Protection Management must be published on www.fpt-software.com. Under contact on www.fpt-software.com the contact details of the Global Protection Officer must be published.

2.2.2 Consent to data processing

Data can be processed following consent by the data subject. Before giving consent, the data subject must be informed in accordance with this Data Protection Policy. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can be given verbally. The granting of consent must be documented.

2.2.3 Data processing pursuant to legal authorization

The processing of personal data is also permitted if national legislation requests, requires or allows this. The type and extent of data processing must be necessary for the legally authorized data processing activity and must comply with the relevant statutory provisions.

2.2.4 Data processing pursuant to legitimate interest

Personal data can also be processed if it is necessary for a legitimate interest of FPT Software. Legitimate interests are generally of a legal (e.g., collection of outstanding receivables) or commercial nature (e.g., avoiding breaches of contract). Personal data may not be processed for the purposes of a legitimate interest if, in individual cases, there is evidence that the interests of the data subject merit protection, and that this takes precedence. Before data is processed, it is necessary to determine whether there are interests that merit protection.

2.2.5 User data and internet

If personal data is collected, processed, and used on websites or in apps, the data subjects must be informed of this in a privacy statement and, if applicable, information about cookies. The privacy statement and any cookie information must be integrated so that it is easy to identify, directly accessible and consistently available for the data subjects.

If use profiles (tracking) are created to evaluate the use of websites and apps, the data subjects must always be informed accordingly in the privacy statement.

If websites or apps can access personal data in an area restricted to registered users, the identification and authentication of the data subject must offer sufficient protection during access.

All technical measures currently taken see chapter 4, Technical Measures.

2.3 Employee Data

2.3.1 Data processing for the employment relationship

In employment relationships, personal data can be processed if needed to initiate, carry out and terminate the employment agreement. When initiating an employment relationship, the applicants' personal data can be processed. If the candidate is rejected, his/her data must be deleted in observance of the required retention period, unless the applicant has agreed to remain on file for a future selection process. Consent is also needed to use the data for further application processes or before sharing the application with other FPT Software legal entities.

In the existing employment relationship, data processing must always relate to the purpose of the employment agreement if none of the following circumstances for authorized data processing apply.

If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding national laws must be observed. In cases of doubt, consent must be obtained from the data subject.

There must be a legal authorization to process personal data that is related to the employment relationship but was not originally part of performance of the employment agreement. This includes legal requirements, collective regulations with employee representatives, consent of the employee, or the legitimate interest of the company.

2.3.2 Data processing pursuant to legal authorization

The processing of personal employee data is also permitted if national legislation requests, requires or authorizes this. The type and extent of data processing must be necessary for the legally authorized data processing activity and must comply with the relevant statutory provisions. If there is some legal flexibility, the interests of the employee that merit protection must be taken into consideration.

2.3.3 Collective agreements on data processing

If a data processing activity exceeds the purposes of fulfilling a contract, it may be permissible if authorized through a collective agreement. Collective agreements are pay scale agreements or agreements between employers and employee representatives, within the scope allowed under the relevant employment law. The agreements must cover the specific purpose of the intended data processing activity and must be drawn up within the parameters of national data protection legislation.

2.3.4 Consent to data processing

Employee data can be processed upon consent of the person concerned. Declarations of consent must be submitted voluntarily. Involuntary consent is void. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In certain circumstances, consent may be given verbally, in this case it must be properly documented. In the event of informed, voluntary provision of data by the relevant party, consent can be assumed if national laws do not require express consent. Before giving consent, the data subject must be informed in accordance with this Data Protection Policy.

2.3.5 Data processing pursuant to legitimate interest

Personal data can also be processed if it is necessary to enforce a legitimate interest of FPT Software. Legitimate interests are generally of a legal (e.g., filing, enforcing or defending against legal claims) or financial (e.g., valuation of companies) nature.

Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the employee merit protection. Before data is processed, it must be determined whether there are interests that merit protection.

Control measures that require processing of employee data can be taken only if there is a legal obligation to do so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. The justified interests of the company in performing the control measure (e.g., compliance with legal provisions and internal company rules) must be weighed against any interests meriting protection that the employee affected by the measure may have in its exclusion and cannot be performed unless appropriate. The legitimate interest of the company and any interests of the employee meriting protection must be identified and documented before any measures are taken. Moreover, any additional requirements under national law (e.g., rights of co-determination for the employee representatives and information rights of the data subjects) must be taken into account.

2.3.6 Telecommunications and Internet

Telephone equipment, e-mail addresses, intranet, and internet along with internal social networks are provided by the company primarily for work-related assignments. They are company tools and company resources. They can be used within the applicable legal regulations and internal company policies. In the event of authorized use for private purposes, the laws on secrecy of telecommunications and the relevant national telecommunication laws must be observed if applicable.

There will be no general monitoring of telephone and e-mail communications or intranet/ internet use. To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented for the connections to the FPT Software network that block technically harmful content or that analyze the attack patterns. For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and internal social networks can be logged for a temporary period. Evaluations of this data from a specific person can be made only in a concrete, justified case of suspected violations of laws or policies of FPT Software. The evaluations can be conducted only by investigating departments while ensuring that the principle of proportionality is met. The relevant national laws must be observed.

2.4 Access Request of state/government or federal agency or other regulatory body

Requests for Personal Data Access of state/government or federal agency or other regulatory body are handled in the same way and under the same conditions as international data transfer by strictly following the requirements of the national law of the respective country. All access requests are register in the access request register. All requests are managed by the GDPO and are subject to agreement with the FPT Software board member responsible for data protection (CFO). The GDPO is responsible for the communication with state/government or federal agency or other regulatory body. The GDPO is responsible for the access request register.

2.5 Policy Review and Evaluation

This policy must be reviewed and evaluated twice a year to reflect the latest status of international standards, legal regulations, technologies, and businesses, and to ensure the timeliness of personal data management practices (see Guideline_Personal Data Protection Policy Development_v2.4).

2.6 Announce and Release

This policy is based on an announcement process that will enable personnel to understand the relevant principles and provisions of the personal data protection management policy so that they can follow it.

This policy must be revised and reviewed by the Personal Data Protection Working Group, approved by the Global Data Protection Officer and the responsible FPT Software board member (CFO). The Global Data Protection Officer is responsible for implementation and internal audits.

3. DATA PROTECTION CONTROL

Compliance with the Data Protection Policy and the applicable data protection laws is checked annually with data protection audits and other controls. The performance of these controls is the responsibility of the Data Protection Representatives. The results of the data protection controls must be reported to the Global Data Protection Officer and the responsible FPT Software board member (CFO). On request, the results of data protection controls will be made available to the responsible data protection authority. The responsible data protection authority can perform its own controls of compliance with the regulations of this Policy, as permitted under national law.

4. TECHNICAL AND ORGANIZATIONAL MEASURES

As non-public company processing Personal Data within a scope of an agreement for commissioned data processing, the FPT Software must take technical and organizational procedures to ensure the compliance with the European Data Protection Regulation and other international Data Protection laws. On top of such procedure, confidentiality, integrity, availability and resilience of systems and components must be guaranteed by FPT Software.

The following groups of measures tackle all aspects of current minimum-security level. They aim at assessing FPT Software's level of data protection when processing personal data on behalf of the Controller. If FPT Software connects to the Controller's systems, FPT Software must complete at least the confidentiality part, whereby FPT Software will need to have the access and access authorization controls as well as the segregation of duties controls completed (sections b) c) d) below).

Below the technical and organizational measures currently realized within FPT Software. A continuous improvement process is implemented:

1. Confidentiality

a) Access Control / Building Security

The aim of the Access Control is to prevent unauthorized use of data processing systems which are used for the processing and the use of Personal Data.

Each employee's user master data and individual identification code are registered in the contact directory. Admission to the data processing systems is only possible after identification and authentication by using the identification code and the password for the particular system.

☒ Alarm system

☒ Automatic access control system

- ☒ Locking system with code lock
- ☐ Biometric access control
- ☐ Light barriers / motion sensors
- ☒ Key transfer regulation (hand-over of keys etc.)

☒ Recording visitors

☒ Commitment of special selected security

☒ Protection of building shafts

☒ Access control by chip card transporter

☒ Manual locking system

☒ Video surveillance of entrances

☒ Safety locks

☒ Identity check by janitor/reception

☒ Commitment of special selected cleaning staff

☒ Commitment to wear authorization card staff

b) Physical Access Control/ System Protection

The aim of the Physical Access Control is to prevent unauthorised people from physically accessing such data processing equipment which processes or uses Personal Data.

Due to their respective security requirements, business premises and facilities are subdivided into different security zones with different access authorizations. They are monitored by security personnel.

Access to special security areas such as the service centre for remote maintenance or ODC is additionally protected by a separate access area. The constructional and substantive security standards comply with the security requirements for data centres.

☒ Internal access control

☒ Strong password specification

☒ Authentication a username/password

☒ Locking server housing/computers

☒ Locking external interfaces (USB etc.)

☒ Intrusion detection system

☐ Encryption of smartphone content

☒ Encryption of data media on laptop computers

☐ Or else, please specify:

☒ Isolation control (permission for user rights)

☐ Biometric authentication

☒ Assignment of user profiles to IT Systems

☒ Use of VPN technology (remote access)

☒ Encryption of mobile data media

☐ Central smartphone administration (e.g., remote deletion)

☐ Secure passwords for smartphones

☒ Assignment of individual usernames

c) Electronic Access Control/Securing Access Authorization

Measures regarding Electronic Access Control are to be targeted on the fact that only such data can be accessed for which an access authorization exists, and that Personal Data cannot be read, copied, changed, or deleted in an unauthorized manner during the processing, use and after the saving of such data.

Access to data necessary for the performance of the particular task is ensured within the systems and applications by a corresponding role and authorization concept.

☒ Rights authorization concept

☒ Number of system administrators "reduced to a minimum"

☒ Logging of system access events, especially entries, changes and deletions of data

☒ Physical deletion of media prior to reuse

☒ Secure storage of data carriers

☒ Encryption of data carriers

☒ Application of hardware firewall

☐ Or else, please specify:

☒ Rights management by system administrator

☒ Recording of deletion

☒ Application of virus protection

☒ Application of software firewall

☒ Password policies (incl. defined password length, password changes)

☒ Use of appropriate shredders resp. specialized service providers

☒ Proper destruction of data carriers

☒ Access logs

d) Separation control/Measures to safeguard the separation of purposes for which Personal Data have been collected

The aim of the Separation Control is to ensure that data which have been collected for different purposes can be processed separately.

Personal Data is used by the Processor for internal purposes only. A transfer to a third party such as a Sub-Contractor is solely made under consideration of contractual arrangements and European Data Protection Regulation.

Processor’s employees are instructed to collect, process, and use Personal Data only within the framework and for the purposes of their duties (e.g., service provision). At a technical level, multi-client capability, the separation of functions as well as the separation of testing and production systems are used for this purpose.

☒ Physically separate storing using separate systems or data carrier

☒ Definition of an authorization concept

☒ Division between productive and testing systems

☒ Encryption of data records, processed for the same purpose

☒ No productive data in testing systems

☒ Logical client separation (software based)

☐ Or else, please specify:

e) Pseudonymizing

The processing of Personal Data in such a way that the data cannot be associated with a specific Data Subject without the assistance of additional information, provided that this additional information is stored separately, and is subject to appropriate technical and organizational measures. See Guideline_Pseudonymisation Minimisation and Encryption_v1.4.1.

☒ Pseudonymously (or anonymous) processing of data

☒ Separation of assignment file and storage in a separate, secure IT system

2. Integrity

a) Data Transfer Control/Data Transfer Security

The aim of the Data Transfer Control is to ensure that Personal Data cannot be read, copied, changed, or deleted without authorization during their transfer and that it can be monitored and determined to which recipients a transfer of Personal Data is intended.

The transfer of Personal Data by FPT Software to a third party (e.g., customers, sub-contractors, service provider) is only made if a corresponding contract exists, and only for a specific purpose. If Personal Data is transferred to companies with their seat outside the EU/EEA or the original country, FPT Software provides that an adequate level of data protection exists at the target location or organization in accordance with the European Union's Data Protection Regulation, e.g., by employing contracts based on the EU model contract clauses.

☒ Establishment of dedicated lines resp. VPN-tunnel

☒ Email encryption

☒ Recording of data recipients as well as periods of scheduled transmission resp. agreed deletion periods

☒ Physical transport: selection of special transport staff and carrier

☐ Or else, please specify:

☒ Data transfer in an anonymous or pseudonymous way

☒ Creation of an overview of regular data request as well as data transfer

☒ Physical transport: Use of secure transport containers/-packing

☒ Use of encrypted external devices when transferring data (CD, USB, stick etc.)

b) Input control

The aim of the Input Control is to make sure with the help of appropriate measures that the circumstances of the data entry can be reviewed and monitored retroactively.

System inputs are recorded in the form of log files. By doing so, it is possible at a later stage to review whether and by whom Personal Data was entered, altered or deleted

☒ Creation of an overview proving which application entitles to input, modify or remove which data

☒ Permission settings to entitle to input, modify and delete data in accordance with a right allocation concept

☒ Continual logging of inputs, modification and deletion of data

☒ Use of individually assigned usernames to ensure access control or input, modification or deletion of data

☒ Retention of a filing system to evaluate the origin of data transmitted to automatically processed data

☒ Activity logs

☐ Or else, please specify.

3. Availability and Resilience

a) Availability control and protection to prevent accidental or willful destruction or loss

The aim of the availability control is to ensure that Personal Data is protected against accidental destruction and loss.

If Personal Data is no longer required for the purposes for which it was processed, it is deleted promptly. It should be noted that with each deletion, the Personal Data is only locked in the first instance and is then deleted for good with a certain delay. This is done to prevent accidental deletions or possible intentional damage.

☒ Server rooms equipped with air conditioning

☒ Server rooms equipped with protective plugs

☒ Server rooms equipped with fire extinguishers

☒ Back-ups stored separately in a safe place

☒ Emergency plan

☒ Business continuity plan

☒ No server rooms below sanitary facilities

☒ Regular data file back-ups

☒ Supervision emergency plan

☐ Or else, please specify:

b) Rapid Recovery

☒ Recovery acc, back-up and recovery concept

☒ Recovery testing

☒ Supervision emergency plan

4. Procedures to handle regular review, valuation and evaluation

a) Data Protection Management

☒ The principles relating to processing of personal data (collection, processing or use) are subject to an internal company policy

☒ The data protection officer has been designated in written form

☒ Employees are committed to data confidentiality/handling of personal data

☒ Employees are committed to comply with the regulations regarding the secrecy of telecommunications

☒ An internal list of processing operations is available. See Guideline_Personal Data Inventory Management_v3.4

☒ The data protection officer is involved in the data protection impact assessment

☒The data protection officer is member of the organizational chart

☒ Employee training courses. See Policy_Personal Data Protection Training_v1.4

☒ Implementation of a control system designed to detect unauthorized access to personal data

☐ Or else, please specify:

b) Incident Response Management

It corresponds to incident management in case of detected or suspected security incidents resp. failure related to IT sectors.

☒ Processing scheme for incident management

☒ Team practicing realistic exercises

☒ Security team designated and trained

☐ Or else, please specify:

c) Data protection by implementation of appropriate technical measures and privacy by default settings (as per EU Regulation)

☒ Adherence to privacy by Design/data protection by appropriate technologies

☒ Selection of privacy-enhancing technologies for future requirements

☒ Adherence to privacy by Default/data protection by appropriate settings

☐ Or else, please specify:

d) Supervision/Engagement of sub-contractors

No data processing is to be carried out without prior specific authorization of the Controller, e.g. clear contractual obligation, formalized order management, strict selection of the service provider, obligation for advance verification, follow-up inspection.

☒Selection of (sub)contractors subject to professional diligence (in particular with regard to data security)

☒ Guidelines drawn up for processor documented in writing (e.g. by data processing agreement)

☒ Processor designated data protection officer (if necessary)

☒ Effective controller's supervision rights agreed

☒ Prior to engagement, verification of security measures recorded by sub-contractor

☒ Processor's employees are committed to sign a secrecy/confidentiality agreement

☒ Ensure erasure or destruction of data after termination of the contract

☒ Continuous review of processor and his activities

☐ Or else, please specify:

5. PERSONAL DATA PROTECTION TRAINING

Every new employee must join the first day Personal Data Protection training.

For every employee processing personal data, it is mandatory to join the Personal Data Protection training on e-campus (FPT Software Training Platform) including a successful exam before starting personal data processing. An annually refresh training is also mandatory.

For every PM, DM, SDM, team lead involved in processing of personal data, it is mandatory to join the extended Personal Data Protection training on e-campus (FPT Software Training Platform) including a successful exam before starting personal data processing. An annually refresh training is also mandatory (see Policy_Personal Data Protection Training_v1.4.1).

FPT Software VN will provide a download version of all training material to each FPT Software legal entity and subsidiary.

6. GLOBAL DATA PROTECTION OFFICER

The Global Data Protection Officer, being internally independent of professional orders, works towards the compliance with national and international data protection regulations. He is responsible for the Data Protection Policy and supervises its compliance. The Global Data Protection Officer is appointed by the FPT Software Board.

The data protection representatives shall promptly inform the Global Data Protection Officer of any data protection risks.

Any data subject may approach the Global Data Protection Officer, or the relevant data protection representative, at any time to raise concerns, ask questions, request information, or make complaints relating to data protection or data security issues. If requested, concerns and complaints will be handled confidentially.

If the data protection representative in question cannot resolve a complaint or remedy a breach of the Policy for data protection, the Global Data Protection Officer must be consulted immediately. Decisions made by the Global Data Protection Officer to remedy data protection breaches must be upheld by the management of the company in question. Inquiries by supervisory authorities must always be reported to the Global Data Protection Officer (see Template_DPO Job Description_v1.3.1).

Article 28 of PDPD VN 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.

Contact details for the Global Data Protection Officer and staff are as follows:
FPT Software Company, Ltd.
Global Data Protection Officer, Michael Hering
F-Town Building 3, Saigon Hi-Tech Park, Lot T2, D1 Street, Tan Phu Ward, Thu Duc City,
Ho Chi Minh City, Vietnam
Cell: +84 90 2606236
E-mail: michael.hering@fpt.com

7. RESPONSIBILITIES AND DISCIPLINARY

The executive bodies of FPT Software, subsidiaries and legal entities are responsible for data processing in their area of responsibility. Therefore, they are required to ensure that the legal requirements, and those contained in the Data Protection Policy, for data protection are met (e.g., national reporting duties). FSU leads, OB heads and managing directors of a legal entity are responsible for ensuring that organizational, HR and technical measures are in place so that any data processing is carried out in accordance with data protection. Compliance with these requirements is the responsibility of the relevant employees. If external agencies perform data protection controls, the Global Data Protection Officer must be informed immediately.

The relevant FSU leads, OB heads or managing directors of a legal entity must inform the Global Data Protection Officer as to the name of their data protection representative. The data protection representatives are the contact persons on site for data protection. They must perform checks and must familiarize the employees with the content of the data protection policies. The relevant management is required to assist the Global Data Protection Officer and the data protection representatives with their efforts. FSU’s, OB’s or legal entities must inform the data protection representatives in good time about new processing of personal data. For data processing plans that may pose risks to the individual rights of the data subjects, the Global Data Protection Officer must be informed before processing begins. This applies in particular to extremely sensitive personal data. The managers must ensure that their employees are sufficiently trained in data protection (annually awareness training with exam, extended training for PM, DM, BU leads).

Improper processing of personal data, or other violations of the data protection laws, can be criminally prosecuted in many countries, and result in claims for compensation of damage. Violations for which individual employees are responsible can lead to sanctions under employment law.
If you do not understand the implications of this policy or how it may apply to you, seek advice from the GDPO via the phone or email (Michael Hering, phone: +84902606236, email: michael.hering@fpt.com).

8. SUPPLEMENTARY GUIDELINES AND DOCUMENTS

PDP Handbook V3.4.1

Policies:

- Policy_Personal Data Protection Training_v1.4.1
- Policy_Privacy Statement_v1.3.1
- Policy_PIMS Scope_v1.3.1

Guidelines:

- Guideline Personal Data Retention v3.4.1
- Guideline Policy Development v2.4.1
- Guideline Personal Data Protection Organization v3.4.1
- Guideline Personal Data Protection Management Audit v2.4.1
- Guideline Complaints and Appeals Handling v3.4.1
- Guideline data breach incident v3.4.1
- Guideline Personal Data Inventory Management v3.4.1
- Guideline Data Flow Mapping v2.4.1
- Guideline Risk Management DPIA v2.4.1
- Guideline_Pseudonymisation Minimisation and Encryption_v1.4.1
- Guideline PII Classification and Rating v3.4.1

Templates:

- Template_DS Consent Withdrawal Form_v1.3.1
- Template_retention schedule_v1.3.1
- Template_audit checklist short_v1.3.1
- Template_internal competence matrix_v1.3.1

- Template_privacy notice register_v1.3.1
- Template_DP Job Description and Responsibilities_v1.3.1
- Template_DPO Job Description_v1.3.1
- Template_DS Request_Incident_Compliant_Appeal_Register-DP_v1.4.1
- Template_Rationale DPO_v1.3.1
- Template_Parental Consent Withdrawal Form_v1.3.1
- Template_Data Subject Right Request Form_v2.4.1
- Template_Parental Consent Form_v1.3.1
- Template_Data Subject Consent Form_v2.4.1
- Template Personal Data Processing Inventory v2.6.1
- Template Standard Contractual Clauses v2.4.1
- Template Personal Data Protection Exhibit v1.6.1
- Template risk management DPIA v3.4.1
- Checklist Before Engagement v3.4.1
- Template Data Processing Agreement v1.3.1
- Template_Non Conformance Report_v1.2.1
- Template_Internal Audit Report_v1.2.1
- Template_Internal Audit Schedule_v1.2.1

Procedures:

- Procedure_Privacy_V1.3.1
- Procedure_DS_Access Request_V1.3.1
- Procedure_Complaints_V1.3.1
- Procedure_Consent Withdrawal_V1.3.1

- Procedure_Consent_V1.3.1
- Procedure_Data Protection Impact Assessment_V1.3.1
- Procedure_Personal Data Breach Notification_V1.3.1
- Procedure_Communication_V1.3.1
- Procedure_Personal Data Transfer_V1.3.1
- Procedure_Data Portability_V1.3.1
- procedure_Third Party Service Contracts_V1.3.1
- Procedure_Sub Contracted Processing_V1.3.1
- Procedure_Competence_V1.3.1
- Procedure_DP Management Review_V1.3.1
- Procedure_Retention of Records_V1.3.1
- Procedure_Continual Improvement_v1.2.1
- Procedure_Internal Audit_v1.2.1

Records:

- Data Breach Contact List Q3_2023
- Record_authorities_Key-Supplier_V1.3.1

Every FPT Software employee can find these Guidelines and templates on the platform QMS.

9. EXCEPTIONS

Any exception must be reviewed and approved by Global Data Protection Officer and also approved by the responsible board member of FPT Software (CFO)/Managing Director of a Subsidiary Company/Legal Entity.

10. APPENDIXES

10.1 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

Abbreviations	Description
PIMS	Personal Information Management System
EU	European Union

10.2 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

No	Code	Name of documents
17	PIPL	Personal Information Protection Law of the People's Republic of China and related laws and regulations
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

10.3 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.