Guideline

PERSONAL DATA PROTECTION MANAGEMENT AUDIT

Document Code	12e-HD/SG/HDCV/FSOFT
Version	2.4
Effective date	01-Aug-2023

Contents

RECORD OF CHANGE

No	Effective Date	Version	Change Description	Reason	Reviewer	Final Reviewer	Approver
1	11-May-2020	1.0	Newly issued	Legal requirement	TrangNN4	Michael Hering	HoanNK
2	01-Jul-2020	1.0.1	HITRUST	HITRUST requirement	TrangNN4	Michael Hering	HoanNK
3	19-Oct-2020	1.1	Update sections: 1.4 Related document, 2. Audit checklist	Legal requirement	TrangNN4	Michael Hering	HoanNK
4	01-Oct-2021	2.0	Change section 1.5 to section 1.3 and 1.3 and 1.4 to section 6.1 & 6.2. Add 1.4. Responsibility	Legal requirement	TrangNN4	Michael Hering	HoanNK
5	01-Oct-2021	2.1	1 added; FPT Software Personal Data Protection Handbook and IMS guidelines, 1.2 added: statement_PIMS scope_V1.0, 6.2 added: statement_PIMS scope_V1.0, template_audit checklist short_V1.0	Legal requirement	TrangNN4	Michael Hering	HoanNK
6	01-Apr-2022	2.2	4 changed: F-Town Building 3 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	Biannually revision	LinhDTD1	Michael Hering	HoanNK
7	01-Nov-2022	2.3	Added 6.3. Data Protection Law, Vietnam, Overview. Added 6.2 15 Republic Act 10173 Data privacy Act 2012 Added 4.2 16 Personal Data Protection Act 2010, Malaysia Added 4.2 18 TISAX	Biannually revision	LinhDTD1	Michael Hering	HoanNK

No	Effective Date	Version	Change Description	Reason	Reviewer	Final Reviewer	Approver
8	01-Aug-2023	2.4	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	Biannually revision	LinhDTD1	Michael Hering	HoanNK

1 Introduction

FPT Software Company, Ltd. Corporate Data Protection Policy, guidelines, procedures, checklists, 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, guidelines, procedures, checklists, 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 Personal Data Protection Handbook and IMS guidelines.

1.1 Purpose

It is mandatory for all FPT Software Units, subsidiaries and legal entities to use following Audit checklist personal data protection management for the internal annually personal data protection audit. It is the standardized approach of FPT Software ensures compliance with the principles of national and international data protection laws in force all over the world.

1.2 Application Scope

See Policy_PIMS scope_V1.3.

This process must be used by all departments and functions globally which are involved in personal identifiable information processing.

1.3 Application of national Laws

The Data Protection Policy, 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 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.

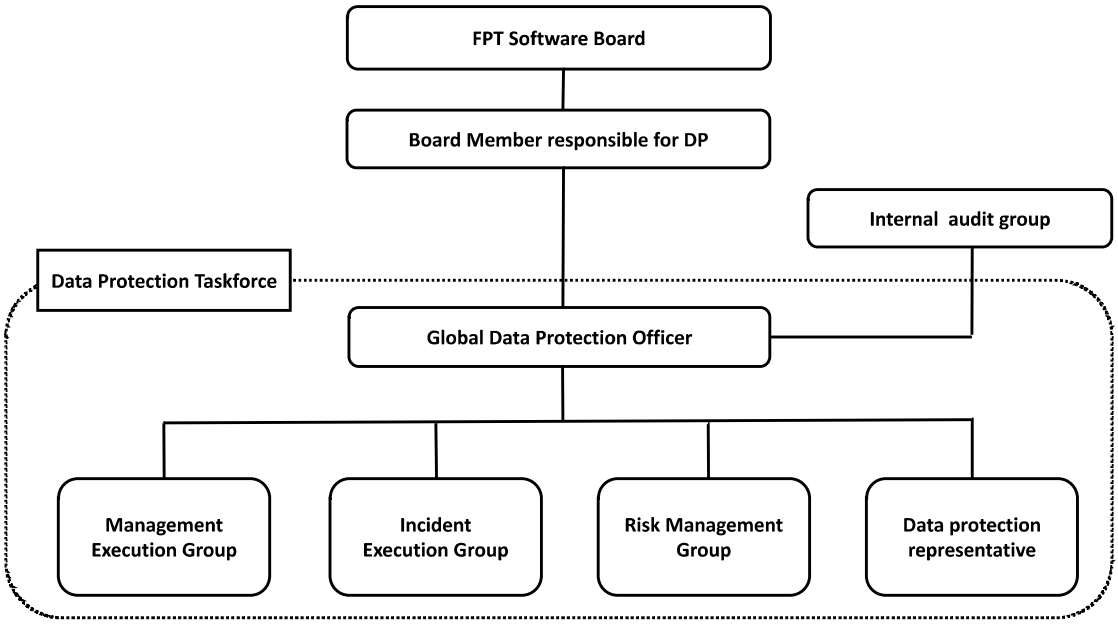
Each subsidiary or legal entity of FPT Software is responsible for compliance with the Data Protection Policy, this guideline, and the legal obligations. If there is reason to believe that legal obligations contradict the duties under the Data Protection Policy or the guidelines, the relevant subsidiary 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 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 and this guideline.

1.4 Responsibility

The Global Data Protection Officer, appointed by the FPT Software Board Member responsible for Data Protection on behalf of the CEO of FPT Software is fully responsible.

The Global Data Protection Officer (GDPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR) and other national laws. The GDPO is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements and other national Personal Data Protection Acts. The primary role of the GDPO is to ensure that organization processes, the personal data of employees, customers, providers, or any other individuals are in compliance with the applicable data protection rules. GDPO should be able to perform the duties independently.

GDPO is responsible for execution or guidance of all data protection audit activities. GDPO must ensure that all departments of the company are following the company guidelines and the respective laws.



More details in Guideline_Personal Data Protection Organization_V3.4.

2 AUDIT CHECKLIST

Status code:

C = 100% compliant I = Improvement in progress N = Not compliant A = Not applicable

Audit area, Accountability and Governance	GDPR Reference	Status				Comment
Do you maintain a corporate data protection policy that demonstrates compliance with requirements including processing, privacy by design and record keeping?	5 (2)					
Did you publish the corporate data protection policy on your company WEB site? Is it available there for customer?						
Did you publish the corporate data protection policy on your intranet? Is it available there for employees?						
Do you train all employees on personal data protection requirements and principles — including processing activities, controls, privacy impact assessments, audits, data subject rights, reporting lines and privacy by design — and the potential impact of noncompliance?	5 (2)					
Do you train all new employees on personal data protection requirements and principles (First Day Training), independent from the future field of work?						
Do you have an extended training for PM, SDM, DM, team leads?						
Do you regularly test, retrain and maintain records of training for employees who handle personal data on their understanding of personal data protection requirements and the company corporate data protection policy?	5 (2)					
Having subsidiaries and legal entities access to the training platform e-campus?						
Global data protection officer (GDPO), does he have reporting authority to the highest level of management, necessary resources, independence, and authority to ensure compliance with the GDPR, APPI, PDPA and other data protection laws?	7 (1) 38 (1-4,6)					

Audit area, Accountability and Governance	GDPR Reference	Status				Comment
Is the GDPO and the local data protection representatives bound by secrecy or confidentiality concerning the performance of his or her tasks?	38 (5)					
DPOs other responsibilities, have they been assessed to avoid conflicts of interest?	38 (6)					
Does the GDPO and the local data protection representatives have the knowledge and ability to fulfil tasks outlined in Article 39?	37(5) 39(1,2)					
Are the GDPO's contact information shared internally, publicly and with the relevant supervisory authority?	37(7)					
Are the unit and local data protection representatives informed about the Personal Data Protection Handbook and the governance model?						
Are the unit and local data protection representatives able to use QMS application?						
Did you sign a data processing agreement with all 3rd parties processing data in your behalf?						
Processing principles						
Are there records management and data retention policies in place and published?	24(1,2,3)					
Do you have documented principles to justify retention periods?	5(1)					
Are personal data processed lawfully, fairly and in a transparent manner?	5(1) 6(1,2,3,4)					
Are all personal data collected for specified, explicit and legitimate purposes, and not further processed in a manner incompatible with those purposes?	5(1)					
Are all personal data relevant, limited and minimized to what is necessary in relation to the purposes for which they are processed?	5(1)					
Are all personal data accurate and kept up to date — and is every reasonable step taken to ensure inaccurate personal data is erased and rectified without delay?	5(1)					
Are all personal data kept only for as long as is necessary for the purposes for which it is	5(1)					

Audit area, Accountability and Governance	GDPR Reference	Status				Comment
processed?						
Are all personal data processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures?	5(1)					
Are clearly identified, detailed, documented and kept up to date the purpose(s) of processing personal data?	5(1)					
FPT Software guiding principles, policy and guidelines are respected and followed?						
Are appropriate technical or organizational measures to ensure security of personal data, including protection against unauthorized processing, accidental loss, destruction or damage implemented?	5(1) 24(1,2)					
Is data protection taken in account at all times, from the moment starting to develop an application to each time personal data are processed?						
Are personal data pseudonymized, anonymized, masked wherever it is possible?						
Are only dummy personal data for testing in use?						
If special categories of sensitive data (revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation) are processed, is compliance with Article 9(2) conditions ensured?	9(1,2)					
Data Subject Rights						
Is it easy for the customers/data subjects to request and receive all the information stored about them?						
Is it easy for the customers/data subjects to correct or update inaccurate or incomplete data?						
Where the accuracy of personal data is	18(1,2)					

Audit area, Accountability and Governance	GDPR Reference	Status				Comment
contested, is processing restricted to enable verification of accuracy?						
Is it easy for the customers/data subjects to request erasure of their personal data?						
Where a data subject requests the erasure of personal data, is taken every reasonable step to erase all data, links and copies without undue delay and when Article 17(1) grounds apply?	17(1,2,3)					
Is it easy for the customers/data subjects to object the processing of their data?						
Is it easy for the customers/data subjects to stop the processing of their data?						
Is it easy for the customers/data subjects to get access to their personal data?						
Is it easy for the customers/data subjects to get a copy of their data for a transfer to another company?						
Where a data subject exercises their right to data portability, the transfer of data to another controller will be done without hindrance, by automated means, and in a common and machine-readable format?	20(1,2)					
Is it easy for the customers/data subjects to get access to the corporate data protection policy?						
Are processes for rectifying inaccurate personal data and having incomplete personal data completed in place and maintained?	16					
Where processing is no longer necessary or lawful, is a process for restricting processing when requested by data subjects in place and maintained?	18(1,2)					
Is it ensured that data subjects who have obtained restriction of processing are informed before restrictions are lifted?	18(3)					
Are all processors, sub-processors and other personal data recipients notified of rectifications, erasures and restrictions of processing?	19					

Audit area, Accountability and Governance	GDPR Reference	Status				Comment
Consent and Notices						
Demonstrate that data subjects have consented to the processing of their data.	7(1)					
Are consent requests clearly distinguishable from other matters, in an intelligible and accessible form, and written in clear and plain language?	7(2)					
Are data subjects asked to positively opt-in (separate and unticked opt-in boxes per Recital 32)?	7(1,2)					
Do data subjects have the right to withdraw consent at any time — and is withdrawing consent as easy and giving consent?	7(3)					
Data Subject Consent Form_V2.0.docx has been used?						
Where processing data of subjects below the age of 16 years, is consent given and authorized by the holder of parental responsibility — and are reasonable efforts made to verify this consent?	8(1,2)					
Are privacy notices and policies clearly provided to data subjects with processor and GDPO contact information, purposes of processing, legal bases for processing, recipients of personal data, international transfers, data retention periods and data subject rights?	13(1,2) 14(1,2)					
Where personal data is not obtained directly from data subjects, do you provide categories of personal data and the originating sources and whether those are publicly accessible?	14(2)					
Are privacy notices and policies provided to data subjects at the time of collection from data subjects or within one month when not obtained from data subjects?	13(1,2) 14(3)					
Are privacy notices and policies provided to data subjects prior to further processing when they have not previously been communicated?	13(3,4) 14(4,5)					
Are all communications with data subjects provided in writing using clear, concise and transparent language?	12(1)					

Audit area, Accountability and Governance	GDPR Reference	Status				Comment
Where information on action taken on data subject rights (Article 15-22) cannot be provided within one month of receipt, do you inform data subjects of the required extension within one month, include reasons for the delay, and extend delivery no more than two months?	12(3)					
Data Breach Management						
Is a breach incident management process, notification policies and procedures in place and maintained?						
Is the guideline_ data_ breach_incident_V3.0.docx known?						
Are all standard processes (QMS application) known?						
Are security measures (e.g., backup, pseudonymization, encryption, testing) implemented and appropriate for data risks?	32(1)					
Is an up-to-date data breach response plan in place and maintained?	33(1,2,3,4)					
For breaches likely to result in a risk to data subjects, do you report the breach to the supervisory authority within 72 hours with categories and the number of subjects concerned, the categories and number of data records concerned, the GDPO's contact information, the likely consequences of the data breach, and measures proposed or taken to address the breach?	33(1,3)					
As a processor, the controller is notified without undue delay after becoming aware of a data breach?	33(2)					
Is a data breach register including facts related to the breach, effects and remedial actions taken in place and maintained?	33(5)					
Are breaches communicated to affected data	34(1,2)					

Audit area, Accountability and Governance	GDPR Reference	Status				Comment
subjects without undue delay and in clear and plain language?						
Awareness and Training						
Did every employee involved in personal data processing the data protection awareness online training including a successful exam?						
How many employees of the department/team have successfully joined the training (number/percentage)?						
Has every new employee joined the first day training?						
Did every PM, DM, SDM, team lead involved in personal data processing the extended data protection online training including a successful exam (number/percentage)?						
Did every PM, DM, SDM, team lead involved in personal data processing the extended data protection classroom training (number/percentage)?						
Is every PM, DM, SDM, team member involved in personal data processing aware of the Data Protection Handbook and QMS?						
Privacy by Design and Default						
Is it ensured that processes are in place to embed privacy by design and default into projects, to include measures that ensure data minimization, pseudonymization, encryption and the processing of only personal data necessary for specified purposes?	25(1,2) 32(1,4)					
Are personal data automatically protected in any IT system, service, and/or business practice, so that individuals should not have to take any specific action to protect their privacy (anonymization, masking, encryption)?						
Are data protection an essential component of the core functionality of your processing						

Audit area, Accountability and Governance	GDPR Reference	Status				Comment
systems, applications and services?						
Are data protection issues considered as a part of the design and implementation of systems, services, products and business practices?						
Is the access to personal data restricted to only those employees processing the data?	24(1) 25(1,2)					
Are there frequently audits and tests of systems and services to ensure ongoing confidentiality, integrity, availability and resilience?	32(1)					
Is it ensured that processes and systems can be restored in the event of physical or technical incidents?	32(1,2)					
Are backup and restore processes frequently tested?						
Is a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures to ensure the security of the processing in place and maintained?	32(1)					
Are storage and processing methods (e.g., redaction) to hard copies of personal data applied?	24(1,2)					
Are documented data destruction procedures in place and maintained for information that is no longer necessary — and are steps taken to ensure that employees are comply with procedures?	24(1,2) 25(1,2)					
Data Protection Impact Assessment						
Is a data protection impact assessment (DPIA) carried out whenever the use of new technologies is likely to result in high risk to data subjects, decisions from automated processing have a legal impact, processing involves special categories of data referred to	35(1)					

Audit area, Accountability and Governance	GDPR Reference	Status				Comment
in Article 9(1) or 10, or include large-scale systematic monitoring of publicly accessible areas?						
Is the GDPO always involved when carrying out a DPIA?	35(2)					
Does the DPIA contain a systematic description of the envisaged processing operations, the purpose of processing, an assessment of the necessity and proportion of processing in relation to the purposes, an assessment of the risks to rights and freedoms of data subjects, and measures envisaged to address the risks, such as safeguards and security measures?	35(7)					
Where appropriate, the views of data subjects or their representatives on intended processing are sought?	35(9)					
Is there a process in place for detecting changes in risks — and are DPIAs for changed risks reviewed?	35(11)					
Are risks arising from each DPIA mitigated?	36(1,2)					
If risks cannot be mitigated, do you contact the supervisory authority with a list of controller and processor responsibilities, the purposes and means of intended processing, measures and safeguards provided to protect data subjects, the GDPO's contact details, the DPIA and any other requested information?	36(3)					
Are DPIA guidelines and templates in place and maintained?						
Records of Processing						
As a controller employing more than 250 people or processing types of data listed in Article 30(5), are records of processing activities containing the name and contact details of the controller and GDPO, the	30(1,3,5)					

Audit area, Accountability and Governance	GDPR Reference	Status				Comment
purpose of processing, a description of data subject and personal data categories, categories of recipients to whom personal data have been or will be disclosed, international transfers of data, time limits for data erasure, and a description of technical and organizational security measures in place and maintained?						
As a processor employing more than 250 people or processing types of data listed in Article 30(5), are records of processing activities containing the name and contact details of the processor, controller and GDPO; categories of processing carried out on behalf of each controller; international transfers of data; and a description of technical and organizational security measures in place and maintained?	30(2,3,5)					
Is it ensured that records of processing activities are maintained in writing and available to the supervisory authority on request?	30(3,4) 31					
Controller's Obligation						
Are policies and procedures for contracting and conducting due diligence on processors and sub-processors in place and maintained?	24(1,2,3)					
Processor's Obligation						
Are only processors used that ensure protection of data subject rights using appropriate technical and organizational measures?	28(1)					
Are these amendments used in a contract with a sub-processor Amendment_Personal Data Protection Management_V2.0 or Exhibit_Personal Data Protection full size_V2.0?						
As a processor, are you not involving a sub-	28(2)					

Audit area, Accountability and Governance	GDPR Reference	Status				Comment
processor without prior specific and general written authorization from the controller?						
Are all processors/sub-processors governed by a contract that establishes the subject matter of processing, duration of processing, nature and purpose of processing, type of personal data and categories of data subjects, and obligation and rights of the controller?	28(3)					
Do contracts and service level agreements with processors/sub-processors outline international data transfers restrictions, ensure confidentiality from persons processing personal data, ensure deletion or return of personal data to controllers at the end of services, allow controllers and auditors to obtain information necessary for inspections and audits, and include all Article 32 security measures?	28(3)					
Is it ensured that processors are implementing data protection by design and default in all processing activities?	25(1)					
International Data Transfer						
If transferring or disclosing personal information, are the data encrypted and are only really necessary data transferred?	32(1)					
Only secure data transfer methods for all communications (e.g., email, file transfers, website forms, payments) are used?	32(1)					
All international data flows and export mechanisms are identified?	44					
Are international data transfers authorized by the Commission (Article 45) or appropriately safeguarded in addition to preserving data subject rights and legal remedies (Article 46)?	45(1) 46(1,2)					
Do the GDPO/Data Protection Representatives regularly check the Official Journal of the	45(8)					

Audit area, Accountability and Governance	GDPR Reference	Status				Comment
European Union for the commission's withdrawals and changes to data transfer authorizations?						
Are appropriate data transfer safeguards provided for by contractual clauses or provisions inserted into administrative arrangements?	46(3)					
Use of the template: Standard Contractual Clauses_template_101219_V1.2.docx						
If relying on binding corporate rules for data transfers, do you ensure they are legally binding and apply to and are enforced by every member concerned of the group of undertakings, in addition to expressly conferring enforceable rights on data subjects with regard to the processing of their personal data?	47(1)					
Do binding corporate rules specify all items in Article 47(2)?	47(1,2)					
Technical and Organizational Measures						
Are you utilizing established frameworks such as ISO27001, ISO27701 and Cyber Essentials to assess and develop adequate measures?						
Is Asset Management established?						
Are appropriate Remote Access policies in place and maintained?						
Are appropriate Bring Your Own Device (BYOD) policies in place and maintained?						
Are appropriate Clear Desk & Screen policies in place and maintained?						
Are appropriate Secure Disposal policies in place and maintained?						
Is Access Control Management established?						
Is Passwords & Encryptions Management established?						

Audit area, Accountability and Governance	GDPR Reference	Status				Comment
Are all mobile devices/hard disks encrypted?						
Are appropriate IS policies in place and maintained?						
Are appropriate Business Continuity Plans and Disaster Recovery Plans in place and maintained?						
Are BCP and DR frequently tested?						
Are a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing in place and maintained?						

Technical and organizational measures (prefilled minimum requirements)

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

☒ 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:

3. Summary of Audit Results

FPT Software is processing personal data in two ways, first as a data controller data about customer, 3rd party provider and FPT Software employees globally, second as a data processor on behalf of the data controller (customer). In the last case FPT Software is following exactly the instruction of the data controller

4 RECOMMENDATIONS, ADVICE

5 SIGNATRURE, AUDITOR/GDPO

Ho Chi Minh City, DD.MM.YYYY

FPT Software Company, Ltd. Global Data Protection Officer,
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

6 APPENDIXES

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
Data Processing	Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Abbreviations	Description
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.

No	Code	Name of documents
		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
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

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.