Regulation

PERSONAL DATA PROTECTION

Document Code	
Version	**1.0**
Effective Date	

RECORD OF CHANGES

No.	Effective Date	Version	Change Description	Reason for Changes	Reviewer	Approver
1		1.0	Newly Create			

TABLE OF CONTENT

I. GENERAL INFORMATION

1. Purpose

This personal data protection regulation **("Regulation")** is developed and implemented for the purpose of protecting personal data and information security of the Company's customers, employees and partners. This Regulation sets forth general requirements for the Company regarding the collecting and processing of personal data.

2. Scope and subjects of application

This regulation applies at FPT Software Company, Ltd.and member companies of FPT Software according to management standards (hereinafter collectively referred to as "Company").

3. Terminology

- **"Personal data (PD)"** is understood as information in the form of symbols, letters, numbers, images, sounds or similar forms in the electronic environment associated with a specific person or help identify a specific person. PD includes basic PD and sensitive PD, PD that the Company can be collected from Customer's PD, Employee's PD, Current PD;
- **"Customer's personal data"** is understood as the customer's personal information that the Company collects and processes during the transaction process and provision of goods and services to customers.
- **"Employee's personal data"** is understood as the personal information and relatives of the Company's employees that the Company collects and processes during the employee's work at the Company.
- **"Passive personal data"** is understood as personal information that the Company obtains but **NOT** through (i) transaction activities, providing goods and services to the Company's customers, (ii) processing cooperation, transactions, signing and implementation of contracts with the Company's partners, and (iii) the signing and implementation of labor contracts. Passive PD often includes *images, activities, locations collected (eg via cameras, sensors) of people passing through the Group's business stores, office areas... and other similar information.*
- **"Data subject"** is understood as the individual referred by PD
- **"Processing PD"** is one or more activities affecting PD, such as: collecting, recording, analyzing, confirming, storing, editing, publishing, combining, accessing, retrieving, retrieving, encode, decode, copy, share, transmit, provide, transfer, delete, destroy or other related actions.
- **"Personal Data Controller"** is understood as the individual or organization that decides the purpose and method of processing PD. To clarify, the PD Controller includes the unit that does not own the PD source but is allowed to use those PD or is the party that controls the information and data containing those PD.
- **"Personal Data Processor"** is understood as the individual or organization that performs PD processing on behalf of the PD Controller, through a contract or agreement with the PD Controller.
- **Personal Data Controller-cum-Processor"** is the organization or individual that simultaneously decides on the purpose, means and directly handles the PD.
- **"Third party"** is an organization or individual other than the Data Subject, PD Controller, PD Processor, PD Controller-cum-Processor that is authorized to process PD.
- **"Data breach"** is understood as information or information systems being attacked or causing harm, affecting the integrity, security or availability; or a security breach resulting in the destruction, loss, unlawful or unexpected alteration, unauthorized disclosure, or unauthorized access of collected and/or processed information.

4. General principles

4.1 Data Protection Principles

- PD is handled legally, transparently and protected by appropriate measures according to the provisions of this Regulation, and according to the provisions of law.
- All forms of buying and selling PD are strictly prohibited.
- The PD is updated, supplemented accordingly and processed only for the Company's legitimate purposes, and has been declared and approved by the data subject.
- Respect the rights of data subjects regarding their personal information.
- The company is responsible for ensuring information network security for the PD it handles.

4.2 Application

- The information collected and processed by the Company may be owned by Data Subjects in many different countries (Vietnam, United States, Europe, Korea, etc.). In addition, information collected and processed in one country may be transferred to one or more other countries. Therefore, the Company needs to pay attention to complying not only with Vietnamese law but also with the laws of relevant countries, including the General Data Protection Regulation **("GDPR")** when processing information of Data Subjects from foreign countries.
- This regulation is built mainly based on Vietnam's laws on personal data and information security, also including some important provisions of GDPR.
- The regulations only provide directional regulations based on the most basic and direct legal provisions. The Regulations do not include all relevant domestic and foreign laws. Therefore, in case a situation arises that is not covered by this regulation, the unit is requested to proactively contact the person in charge or consult with the Company's legal department, and/or a lawyer if necessary.

II. PRIMARY CONTENT

1. Personal data processing

1.1 Before processing data

Before collecting and processing Data Subject's PD, the Company must obtain consent from the data subject:

- When seeking consent, the Data Subject must be informed about: the purpose, approach, start and end time of processing; type of PD and information about third parties relevant to the purposes of processing.
- Silence or non-response by the Data Subject is not considered consent.
- Information can only be processed and used for purposes other than the original purpose after receiving additional consent from the Data Subject (must take steps to obtain additional consent).
- The Data Subject's consent must be expressed clearly and specifically in writing, voice, checking the consent box, consent syntax via text message, selecting consent technical settings or via another action demonstrates this.

Seeking consent is guided for each subject as follows:

1.1.1 ***For Customer's personal data***: application for approval/additional consent is carried out in accordance with the PERSONAL DATA PROTECTION POLICY publicly posted by the Company or specified in the written agreements signed with the Data Subject. The PD privacy policy template is attached to these Regulations. The company builds appropriate implementation methods for each of its products and services.

For handling Customer's PD to provide marketing services and introduce advertising products, it is necessary to clearly inform Customers of the content, method, form, and frequency of product introduction

1.1.2 ***For Employees' personal data***: seeking consent is carried out according to the EMPOYEE PERSONAL DATA PROTECTION POLICY applied internally. The employee's PD protection policy template is attached to this Regulation.

1.1.3 ***For passive personal data:*** At locations where the Company has the capability to collect and process passive personal data, it is necessary to widely announce it in a reasonable manner, including (i) clearly stating that cameras/sensors are used within areas under company's rights, (ii) has a link (or QR code) referencing the Company's privacy policy. However, even in cases where these notices have been placed, the use of passive PD for commercial purposes should also be carefully considered, and only used for the purpose of ensuring safety and security and legitimate purposes according to the provisions of law.

1.1.4 ***Other regulations:***

a. Data Subject consent is not required in the following cases:
   - In an emergency to protect the life or health of the Data Subject or others.
   - Publicizing PD according to the provisions of law.
   - To perform the Data Subject's contractual obligations with the Company.
   - PD is obtained from audio and video recording activities in public places for the purpose of protecting national security, social order and safety, and the legitimate rights and interests of organizations and individuals according to the provisions of law.
   - Where it is difficult to determine, the Data Subject's consent should be obtained.

b. In case the Company has an agreement allowing a third party to share, access or process the Company's PD, the relevant unit signing the agreement with the partner must ensure that approving the partner to use PD is appropriate for the purpose authorized by the Data Subject and the partner must strictly comply with regulations on PD protection as well as other information security requirements of the Company.

1.2 During the data processing

During data processing, Data Subjects have the right to request provision, access, modification, withdrawal of consent, deletion, restriction of processing, and objection to data processing. When receiving requests to exercise Data Subject rights, the department in charge at each Company should note:

- Make requests, or provide Data Subjects with access to update or amend information themselves, unless otherwise specified.
- After receiving requests for: providing data; restrict data processing; request to object to data processing; or delete data, the department in charge needs to do so within 72 hours.
- When withdrawing consent, it is necessary to notify the Data Subject of the consequences and damages that may occur.
- For requests to rectificating data, if it cannot be done, it is necessary to notify the Data Subject after 72 hours from receipt of the request.
- The company, if there is an activity of collecting and processing personal data, it is necessary to designate a department/personnel in charge of protecting personal data.

1.3 Impact assessment report:

- From the time started processing PD, it is necessary to conducting and storing records assessing the impact of processing PD or the transfer of PD abroad to be ready to serve the inspection and assessment activities of the Ministry of Public Security, according to regulations of the law from time to time.
- Impact assessment documents are carried out according to instructions in Decree 13/2020/ND-CP or other regulations from time to time.

2. Outsourcing data processing

- In case the Company outsources data processing, a contract or agreement with the Processor is required.
- In case the Company processes personal information of foreigners who are citizens of and are living in the European Union and the Company outsources data processing services, the contract with the Processor must contain a number of conditions following Article 28.3 of the GDPR.

3. Data processing log

- The company must record and store system logs of PD processing activities. Depending on the level of each company's information system, the Company can develop corresponding system log standards according to instructions in TCVN 11930:2017 regarding information technology - safety techniques - basic requirements about information system security regulations by level or other regulations.
- *For example,* for a level 2 information system, the system log includes: setting up the function of recording and storing system logs on system devices; utilizing a time server to synchronize time between network devices, endpoints, and other components in the system participating in monitoring activities.

4. Data protection measures

- The company needs to take necessary management and technical measures to protect information from being lost, stolen, disclosed, changed or destroyed. Developing a plan to ensure information security meets basic requirements at each level according to the principles specified in Decree 85/2016/ND-CP dated July 1, 2016 on ensuring information system security by level or other regulations from time to time.

4.1 Management measures

Companies can choose to establish basic requirements for each level of their information system, including:

- Information security policy *(Please see more at FPT Group Data Management Regulations, code 05-QD/TT/HDCV/FPT).*
- Organize information security assurance;
- Ensuring human resources;
- Management of system design and construction;
- System operation management
- Risk management plan for information security;
- Plan for ending operation, exploitation, liquidation and destruction of the information system.

4.2 Technical measures

Companies could choose to establish basic requirements for each level of their information system, including:

- Ensuring network security;
- Ensuring server security;
- Ensuring the safety of users' computers;
- Ensuring application security;
- Ensuring data security.

5. Notification of violations

5.1 Responsibility to Notify

When a data breach is detected, the department in charge must notify the IT department to coordinate handling. In case the level of impact is large, the department in charge coordinates with the IT department to notify the Executive Board of their company.

5.2 Notification of violation

No later than 72 hours after the violation occurs, the Company must notify the Ministry of Public Security - Department of Cyber Security and Crime Prevention using high technology when detecting the following cases:

- Detecting legal violations against PD;
- PD is processed for the wrong purpose, not in accordance with the original agreement between the data subject and the controller, controller cum processor or violates the provisions of law;
- The data subject's rights are not guaranteed or are not implemented properly;
- Other cases as prescribed by law.

Reporting is carried out in accordance with the provisions of Decree 13/2020/ND-CP or other regulations from time to time.

6. Training

People assigned to protect data protection are trained in information security awareness and data protection annually.

III. IMPLEMENTATION ORGANIZATION

1. The Information Technology Department, Human Resources Department, Technology Department, Compliance Monitoring Board of the Group and related units are responsible for implementing and guiding affiliates to build a security protection system at their units, comply with this Regulation and related regulations issued by FPT Group.
2. The President/General Director of affiliates are responsible for implementing the provisions of this Regulation.

FPT SOFTWARE COMPANY LIMITED