*Guideline*

# DATA BREACH INCIDENT RESPONSE

| | |
|---|---|
| **Document Code** | **09e-HD/SG/HDCV/FSOFT** |
| **Version** | **3.4** |
| **Effective date** | **01-Aug-2023** |

# TABLE OF CONTENT

## RECORD OF CHANGE

| No | Effective Date | Version | Change Description | Reason | Reviewer | Final Reviewer | Approver |
|---|---|---|---|---|---|---|---|
| 1 | 21-Oct-2019 | 1.0 | Newly issued | Business requirement | MinhPT | Michael Hering | HoanNK |
| 2 | 11-May-2020 | 2.1 | Update “Introduction” section-Update “Related Documents” sub-section-Change “Data Breach Response Plan” into “Data Breach Response GDPO”-Update “Personal Data Incident Response Plan” sub-section | Update according to annually revision requirement | TrangNN4 | Michael Hering | HoanNK |
| 3 | 01-Jul-2020 | 2.1.1 | HITRUST | HITRUST requirement | TrangNN4 | Michael Hering | HoanNK |
| 4 | 19-Oct-2020 | 2.2 | Update sections: related document, Reasons for Data Breaches<br>Change “Data Breach Contact List Q1_2020” into “Data Breach Contact List Q4_2021” | Legal requirement | TrangNN4 | Michael Hering | HoanNK |
| 5 | 01-May-2021 | 3.0 | Change the document structure.<br>Update sections: Purpose, Related Document<br>Add Responsibility section | Legal requirement | TrangNN4 | Michael Hering | HoanNK |
| 6 | 01-Oct-2021 | 3.1 | 1.2 added: statement_PIMS scope_V1.0, 1.4 added: Guideline_Personal Data Retention_v3.1, Procedure_Retention of Records_V1.0, 2.3 added: template_DS request_incident_compliant _appeal_register-DP_V1.1, DPO Tool, 3.4 replaced Data Breach Contact List Q1_2021 with Record_internal contracts_V1.0, 4.2 replaced Data Breach Contact List Q1_2021 with Record_internal | Legal requirement | TrangNN4 | Michael Hering | HoanNK |
| 7 | 01-Apr-2022 | 3.2 | 4.2 14 added PIPL,<br>4.2 15 added: PDPL, UAR, Decree-Law No. 45 of 2021<br>4.2 17 added: Decree of the Vietnamese Government: Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân<br>4.2 18 PDP_ Handbook_Version_V3.2 | Biannually revision | LinhDTD1 | Michael Hering | HoanNK |

| No | Effective Date | Version | Change Description | Reason | Reviewer | Final Reviewer | Approver |
|---|---|---|---|---|---|---|---|
| 8 | 01-Nov-2022 | 3.3 | Deleted 2.3: From 01.10. 2021 DPO Tool (WEB based application), section incident<br>Added 4.3. Data Protection Law, Vietnam, Overview.<br>Added 4.2 15 Republic Act 10173<br>Data privacy Act 2012<br>Added 4.2 16 Personal Data Protection Act 2010, Malaysia<br>Added 4.2 18 TISAX | Biannually revision | LinhDTD1 | Michael Hering | HoanNK |
| 9 | 01-Aug-2023 | 3.4 | Adjust document version numbers<br>added 4.2 14, 18<br>changed 4.2 22: Came in force 07/2023<br>changed 4.3 PDPD was finalized and was coming in force 07/2023 | Biannually revision | LinhDTD1 | Michael Hering | HoanNK |

# 1 INTRODUCTION

FPT Software Company, Ltd. ("FPT Software" hereinafter) Corporate Data Protection Policy, guidelines, procedures 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 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 ISM guidelines.

Under the EU GDPR (General Data Protection Regulation), organizations must respond to a serious data breach within 72 hours becoming aware of it. This places a significant burden on FPT Software; after all, taking the appropriate measures to comply with the law while simultaneously dealing with the collateral impact of a breach is not an easy task.

## *1.1 Purpose*

The purpose of this guideline is to outline the internal personal data breach reporting procedure of FPT Software, and our internal and external response plan and it should be read in conjunction with our data protection policy Policy_Personal Data Protection Management_V3.4.

Description of Data Breach Incident Response and the contribution of FPT Software's senior management to minimize the risk of a personal data breach or a breach of data subject rights by an efficient Personal Information Management System (hereinafter PIMS).

## *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, procedures 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 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.

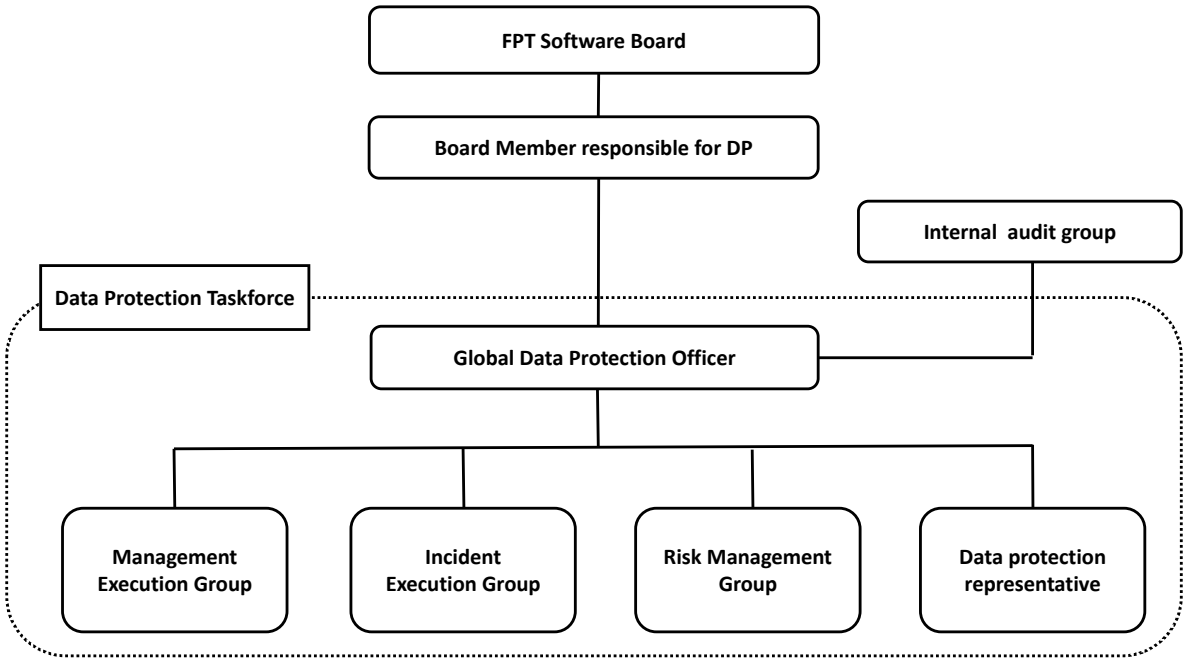
### *1.4 Responsibility*

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 his duties independently.

GDPO is responsible to manage or guide all data breach incident 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. Retention, please see Procedure_Retention of Records_V1.3 and Guideline_Personal Data Retention_v3.4.



# 2 PERSONAL DATA BREACH

A personal data breach is a “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed”.

A breach is therefore a type of security incident and there are three different types of breach that may occur:

1. Confidentiality breach – an accidental or unauthorized disclosure of, or access to, personal data.
2. Availability breach – an accidental or unauthorized loss of access to, or destruction of, personal data.
3. Integrity breach – an accidental or unauthorized alteration of personal data.

A breach can concern confidentiality, availability, and integrity of personal data at the same time, as well as any combination of these.

A personal data breach would, for example, include:

- personal data being disclosed to an unauthorized person, e.g., an email containing personal data being sent to the wrong person.
- an unauthorized person accessing personal data, e.g., an employee’s personnel file being inappropriately accessed by another member of staff due to a lack of appropriate internal controls.
- a temporary or permanent loss of access to personal data, e.g., where a client’s or customer’s personal data is unavailable for a certain period of time due to a system shut down, power, hardware or software failure, infection by ransomware or viruses or denial of service attack, where personal data has been deleted either accidentally due to human error or by an unauthorized person or where the decryption key for securely encrypted data has been lost.

## *2.1 Personal Data Breach Notification*

Not all personal data breaches have to be notified to the Supervisory Authorities. The breach will only need to be notified if it is likely to result in a risk to the rights and freedoms of data subjects, and this needs to be assessed by FPT Software on a case-by-case basis. A breach is likely to result in a risk to the rights and freedoms of data subjects if, for example, it could result in:

- Loss of control over their data
- Limitation of their rights
- Discrimination
- Identity theft
- Fraud
- Damage to reputation
- Financial loss
- Unauthorized reversal of pseudonymization

- Loss of confidentiality
- Any other significant economic or social disadvantage

Where a breach is reportable, FPT Software must notify the Supervisory Authorities without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. If our report is submitted late, it must also set out the reasons for our delay. Our notification must at least include:

- A description of the nature of the breach including, where possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected records
- The name and contact details of FPT Software CEO or the Board member responsible for Data Protection
- The name and contact details of FPT Software Global Data Protection Officer
- A description of the likely consequences of the breach
- A description of the measures taken, or to be taken, by FPT Software to address the breach and mitigate its possible adverse effects.

We can provide this information in phases, without undue further delay, if it cannot all be provided at the same time.

Awareness of the breach occurs when we have a reasonable degree of certainty that a breach has occurred. In some cases, it will be relatively clear from the outset that there has been a breach. However, where it is unclear whether or not a breach has occurred, we will have a short period of time to carry out an initial investigation after first being informed about a potential breach in order to establish with a reasonable degree of certainty whether or not a breach has in fact occurred. If, after this short initial investigation, we establish that there is a reasonable degree of likelihood that a breach has occurred, the 72 hours starts to run from the moment of that discovery.

### *2.2 Data Breach Communication to Data Subjects*

Where the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, FPT Software also needs to communicate the breach to the affected data subjects without undue delay, i.e., as soon as possible. In clear and plain language, we must provide them with:

- A description of the nature of the breach
- The name and contact details of FPT Software CEO or the Board member responsible for Data Protection
- The name and contact details of FPT Software Global Data Protection Officer
- A description of the likely consequences of the breach
- A description of the measures taken, or to be taken, by the Company to address the breach and mitigate its possible adverse effects.

We will also endeavor to provide data subjects with practical advice on how they can themselves limit the damage.

We will contact data subjects individually, by e-mail, unless that would involve FPT Software in disproportionate effort, such as where their contact details have been lost as a result of the breach

or were not known in the first place, in which case we will use a public communication, such as a notification on our website.

However, we do not need to report the breach to data subjects if:

- We have implemented appropriate technical and organizational protection measures, and those measures have been applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person who is not authorized to access them, such as state-of-the-art encryption, or
- We have taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize.

### *2.3 Data Breach Register*

FPT Software maintains a register of all personal data breaches, regardless of whether or not they are notifiable to the Supervisory Authorities. The register will include a record of:

- The facts relating to the breach, including the cause of the breach, what happened and what personal data were affected
- The effects of the breach
- The remedial action we have taken

Data Breach Register until 30.09.2021 based on Template_Data Subject Request Incident Compliant Appeal Register_v1.4.

### *2.4 Data Breach Response Plan*

A data breach response plan is a set of actions that help companies detect and respond to incidents in a fast, planned and coordinated manner. This includes technical measures, such as anti-malware software and data encryption, as well as policies and processes for employees to follow.

An effective plan reduces the financial and reputational damage associated with a breach and helps FPT Software complies with the GDPR or other national and international laws/regulations.

### *2.5 Challenges of a Data Breaches Response plan*

- Identifying a suspected cyber security incident.
  The longer FPT Software is exposed to a vulnerability; the more damage can be caused. As a result, spotting a data breach promptly can be the difference between a moderate disruption and a disaster. This is why information security risk assessments and Data Protection Impact Assessments (DPIA) are so important. They help to detect weaknesses and help to identify appropriate measures to address them.
- Establishing the objectives of an investigation and a clean-up operation.
  It's obviously important to get up and running as soon as possible after a breach, but this should be a coordinated effort. We must review what caused the incident and set goals for what we are aiming to achieve. We might ask, for example, when or whether customers, employees or

data subjects need to be notified, or whether a system needs to be at full capacity before it can go back into use.

- Analyzing all available information related to the potential cyber security incident.
  Potential breaches (or reviews into incidents that already occurred) will generate a lot of raw data. We need to not only know how to use that information but also have adequate personnel and resources to disseminate it.
- Determining what has actually happened.
  Data breaches aren't always clear-cut. Sometimes we will find a malware injection, but often it'll take time to piece together what went wrong. Until we figure this out, we won't be able to review your network for similar mistakes.
- Identifying what systems, networks, and information (assets) have been compromised.
  It's hard to know whether the breach we have identified is the full extent of the damage. A cybercriminal might have launched multiple attacks or leveraged their way into other parts of our systems or applications. As such, we will need to take the time to investigate the incident and review anything that could have been compromised.
- Determining what information has been disclosed to unauthorized parties, stolen, changed, deleted or corrupted.
  It's not only compromised systems, networks, applications, and assets that we need to identify. We must also investigate the information within those systems.
- Finding out who caused the breach and why.
  Most breaches are random attacks by crooks looking for financial gain, but some incidents will target you specifically, such as political attacks or those caused by malicious insiders.
- Working out how the breach happened.

  This is the fundamental question all companies must be able to answer if they are to prevent future attacks. It's all well and good stopping this incident, but if we don't know how to address the root cause, it won't be long before we are back where we started.

- Determining the potential business impact of the cyber security incident or a personal data breach.
  We need to know the financial implications of the breach so we can plan for the long-term. The cost of recovery and the loss in productivity will affect our revenue, may well affect our ability to meet deadlines and may affect our reputation as well contractual obligations.
- Conducting a sufficient investigation using forensics to identify those responsible.
  FPT Software needs to have the capabilities to conduct a forensic investigation, and those must be familiar with the process. However, the process can be essential for discovering clues that could bring the perpetrators to justice.

### *2.6 Reasons for Data Breaches*

There are four fundamental ways data breaches occur:

- Theft or Loss of Physical Equipment
  A data breach can occur with the theft or loss of physical equipment which stores data, such as laptop computers or memory storage devices.
- Illegal access to the systems or information
  A data breach can occur through unlawful access to PII data by technological means such as hacking into existing computer systems or hijacking computers with viruses, worms, or trojans. Once inside a system, criminals can steal data, infect it, or overload computer systems.
- Insiders
  A data breach can be committed by current employees, ex-employees, or even through social engineering where an employee is tricked into providing access or information (phishing is considered to be socially engineered fraud).
- Oversight
  A data breach can occur when no one thought the information needed to be protected and no precautions were taken to safeguard the data in the first place.

### *2.7 Data Breach Response GDPO*

FPT Software's CEO together with the board member responsible for Data Protection has nominated a Global Data Protection Officer (GDPO). He has assembled a team to investigate, manage and respond to the personal data breach (Incident Execution Group). The Incident Execution Group will then:

- Make an urgent preliminary assessment of what data has been lost, why and how.
- Take immediate steps to contain the breach and recover any lost data.
- Undertake a full and detailed assessment of the breach.
- Record the breach in the FPT Software's data breach register.
- Notify the Supervisory Authorities where the breach is likely to result in a risk to the rights and freedoms of data subjects.
- Notify affected data subjects where the breach is likely to result in a high risk to their rights and freedoms.
- Respond to the breach by putting in place any further measures to address it and mitigate its possible adverse effects, and to prevent future breaches.

### *2.8 Data Breach Reporting*

If someone (employee) knows or suspects that a personal data breach has occurred, she/he must immediately both advise the line manager and contact the GDPO. She/he must ensure she/he retain any evidence she/he has in relation to the breach, and she/he must provide a written statement setting out any relevant information relating to the actual or suspected personal data breach, including:

- your name, department and contact details
- the date of the actual or suspected breach
- the date of the discovery of the actual or suspected breach
- the date of the statement
- a summary of the facts relating to the actual or suspected breach, including the types and amount of personal data involved
- what she/he believes to be the cause of the actual or suspected breach?
- whether the actual or suspected breach is ongoing?
- who she/he believes may be affected by the actual or suspected breach?

She/he must then follow the further advice of the GDPO. She/he must never attempt to investigate the actual or suspected breach her/himself and she/he must not attempt to notify affected data subjects. The GDPO will investigate and assess the actual or suspected personal data breach in accordance with the response plan set out below and the Incident Execution Group will determine who should be notified and how.

# 3 GUIDELINE CONTENT

## *3.1 Preparation for a Data Breach*

While theft prevention should always be the primary goal of any organization, proactive planning can minimize the impact when a breach does occur.

There are four main things to keep in mind when the time comes to respond to a data breach –

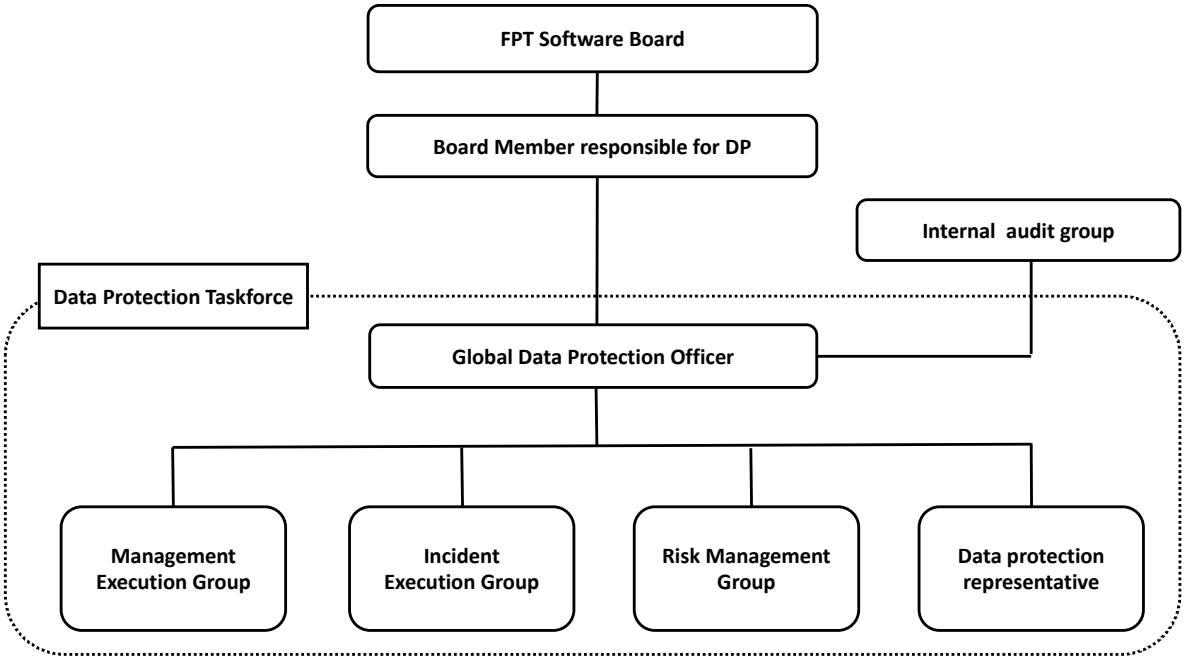
- It is important to move swiftly and follow our completed Data Breach Incident Response Plan.
- It is important to document all ongoing events, all people involved, and all discoveries into a timeline for evidentiary use.
- It is important to entry immediately in the root cause analysis.
- It is important to start immediately with the deployment of risk mitigation measures.

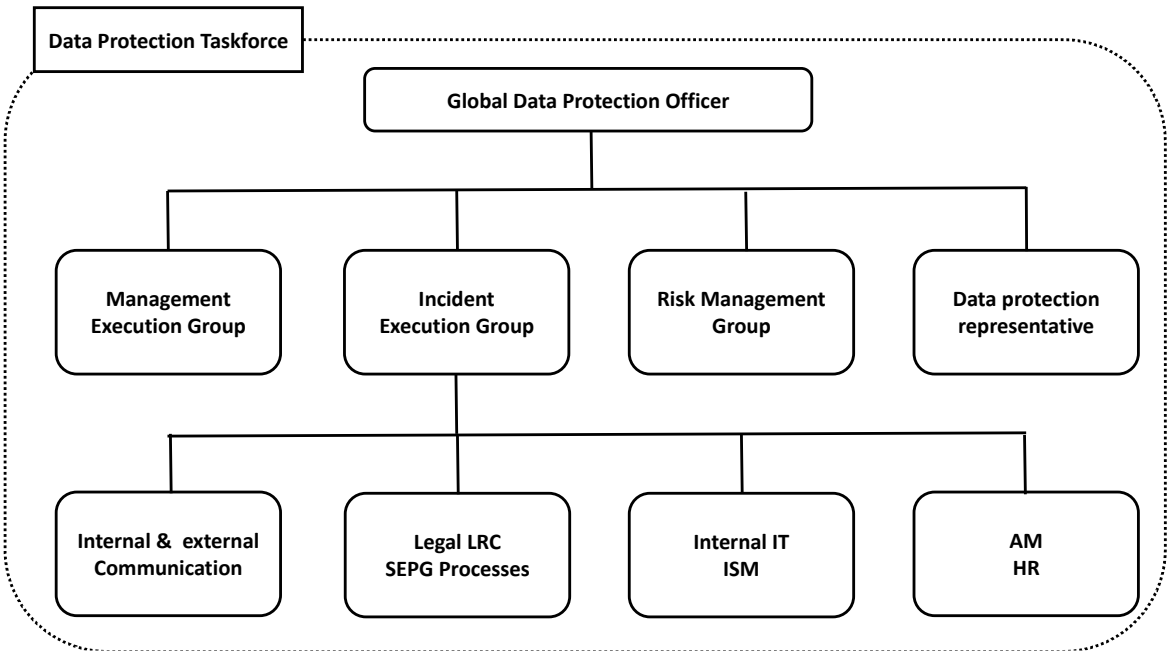
The following is a list of actions that are going to need to be taken when a breach occurs:

- Identify how the breach happened, contain the breach, and implement a solution so that it cannot happen again (Root cause analysis, breach impacts, appropriate measures implementation).
- Notify appropriate people within FPT Software, subsidiaries and legal entities.
- Notify External involved parties, within required time frames, such as:
    - Data subjects
    - Data controller
    - Contract partner
    - Data protection authorities

### *3.2 Data Breach Incident Management*

## Incident Management, Data Breach Respond Organization



FPT Software have established a strong team with the right mix of expertise:

- GDPO
- Legal, Risk and Compliance LRC
- Processes, SEPG
- Internal IT
- Information Security
- Account management
- HR
- Communication

In the case of a data breach incident an Incident Lead will be assigned to direct and manage the Incident Execution Group (internal response team), as well as to act as the go-between for GDPO/FPT Software Board Member responsible for DP and the Incident Execution Group. This individual should be considered to be the project lead for the breach incident. The other members of the Incident Execution Group have specific responsibilities to protect our company, customers, and data subjects but all of them report directly to the Incident Lead. For all significant data breach incidents (high severity level) with high range of coverage the GDPO will take over the role of the Incident Lead, for minor incidents the data protection representative of the respective FPT Software unit. This person will coordinate efforts among all groups, notify all the appropriate people within the company and externally, and create the documentation and timeline of activities, identify key tasks, and estimate costs.

GDPO and FPT Software Board Member responsible for DP must be kept up to date during a data breach incident. The Incident Lead will be running tactical, day-to-day operations of the data breach as well as regularly updating management.

Internal & external communications group must be involved in every personal data breach incident. A decision will need to be made very early in the event to determine whether or not it is appropriate to notify customer, data controller, data subject or supervisory authority of the incident. If someone needs to be notified, it is critical to begin notification in a timely manner. Every country/state has different notification laws based on the kind of personal data information that was breached, and communications groups must work hand-in-hand with legal LRC and the GDPO to determine the specific legal obligations and timeline for notification.

Legal LRC, processes SEPG group works with GDPO to find out what is required in the response. They are responsible for determining whether or not customer, data controller, data subject or supervisory authority should be notified and the legal requirements around what the notification must include.

Internal IT and ISM teams are critical in helping identify what information was actually compromised.

### *3.3 Personal Data Breach Checklist*

If a personal data breach happens, timing is everything. Everything that happens, everything what is discovered must be documented, and turn it into a timeline. Within the first few hours after discovering a potential personal data breach, it is important to start to run through the following checklist:

Development of a Personal Data Breach Incident investigation including the following:

- Date/Time of discovery of the personal data breach
- Name of person reporting the personal data breach
- Name of the data subject notifying an unlawful personal data processing
- Details of how the personal data breach was detected and reported
- Type of data breach: theft, illegal access, insiders, oversight, data lost, data corrupted
- Root cause of the breach.
- Description what happened
- Could the breach be contained (how and when)?
- Technical and/or organizational measures implemented, so it cannot happen again (time and date)?
- How many data subjects are affected?
- What kind of data subjects are affected? (Employees, customers, other)
- What kind information, data was lost? (Be very specific with this list, for example, “Did every name lost including a smart meter number? Is there a relation to an invoice number, to an address and so on?

Development of a list of all external officials and individuals contacted and involved in the incident:

- Clients/customer
- Data controller
- Data processor/ Data sub processor
- Supervisory Authorities

Identification of the issue – type of Personal Data incident:

- Network/server breach/Cloud
- Storage system breach
- Hardware loss, theft, or destruction
- Software loss, theft, or destruction
- Hacking/unauthorized third-party access to a system or application
- Unauthorized websites that publish sensitive corporate information not approved for public consumption

What business rules and processes are affected?

Assigning of an incident number or assigning an existing incident number and reactivation (if necessary)

Assigning new incidents, alert the Incident Lead

Information of the GDPO

Activation of the Incident Execution Group (Main goal: Maintain and restore business continuity)

The Incident Execution Group should:

- Collect and/or review the incident documentation and event reports
- Verify as facts
- Assign event severity
- Alert appropriate external and internal contacts

Maintain a complete chain of evidence

Record any and all modifications

Restrict information – keep it on a need-to-know basis only

Secure the area and record the information (gather names and contact information of everyone, restrict the area, notate all physical security controls)

Begin collecting evidence

Use the Data Breach Investigations Log

Protect the host servers (Involve Internal IT and ISM, if necessary, a certified data forensics agency to perform or assist the investigation)

Restore the host servers (use appropriate monitoring)

Maintain data integrity -- maintain baselines of normal activity to use for comparison

Start forensic analysis – how, what, why did this happen?

Keep detailed logs

Be consistent with the way you collect and record information throughout the investigation

Consult legal LRC

Develop and record a hypothesis:

- How does the evidence support/contradict it?
- What did you do, what evidence did you find, and how did you test the hypothesis?
- What important interactions took place?
- Were there any other ideas at the time?
- Record anything else that helps the FPT Software collectively remember things accurately

Keep the evidentiary chain intact for all electronic and physical evidence

Treat every incident as if it will lead to a court case (include the time and date for each entry in your notes and sign every page)

Remember, all information can become available to lawyers through the information discovery and could become public.

Do not include confidential information unless necessary

Begin the process of reporting the incident

Limit communication to Incident lead, line manager, GDPO

Use discretion when sharing information

Incident lead must create Executive-Level Report (approximately 1-2 pages) approved by the GDPO including:

- High-level description of the incident and its scope

- Impact on the FPT Software
- Actions taken to prevent further occurrences
- Recommendations for further action

As well a Technical Report must be created approved by the GDPO that including:

- Detailed information about the breach
- Detailed information about the investigation
- Detailed information about technical and organizational measures taken
- All conclusions reached
- Data used in the report should reference collected evidence and must be verifiable

Keep all evidence, logs, and data associated with the incident
Put limited access applications and systems, secure storage
Give original records to Legal LRC and save a copy for company security records
Grant access to the storage facility only to incident investigators, incident execution group and the GDPO
Records should be kept of all access granted to the storage facility
Create an itemized inventory of all the evidence, verify it with LRC, and have that representative sign and date the inventory list for the records
Use the Data Breach Investigations Log to record the findings of each investigation – it helps create a useful record of events, which can help with Supervisory Authority cases and can help future reactions and prevention of similar events.

### *3.4 Personal Data Incident Response Plan*

This Chapter guides to a tailored Incident Response Plan. The worksheets serve as a guide to you proper documentation of events, actions, and timelines. Maintain this plan with other documentation so that the source of an incident can be identified and traced. So, that the information is immediately available if needed.

Also following copies should be maintained:

- FPT Software IMS Incident Response Plan
- Service and Operating Level Agreements
- Data Security standard document, ISM policies
- Personal data protection policies
- Software inventory with licensing information
- Asset and hardware inventory

An employee who becomes aware of a suspected or actual personal data breach must inform the GDPO and the line manager by email and by phone call without delay. The email address for contacting the

GDPO is michael.hering@fsoft.com.vn and the email account should be regularly reviewed by the GDPO.

The line manager must get in contact with the GDPO immediately to decide further actions. Based on nature of the breach/incident and the risk level, the GDPO assign an incident lead and the incident execution group (depending on country/region, system owner, data owner).

The incident execution group must describe the nature of the incident by using the response plan template and must maintain the incident log. The Incident lead must create Executive-Level Report (approximately 1-2 pages) approved by the GDPO. A Technical Report must be created by the system owner/IT approved by the GDPO. A Risk assessment and risk mitigation (immediately measure) must be done system/data owner approved by the GDPO.

Information of FPT Software board by GDPO.
Communication with data subjects and Supervisory Authorities leaded by the GDPO, if it is necessary.
GDPO must prove if the agreed measures are sufficient and has to decide follow-up actions.
GDPO must guide the lesson learnt session.

GDPO creates the final incident report to approve by the board member responsible for DP (CFO).

**Response plan template**

| **Incident Execution Group** | |
|---|---|
| Global Data Protection Officer: | |
| Incident Execution Group lead: | |
| Members of Incident Execution Group: | |
| **Background** | |
| Name and department/Unit/OB of person notifying actual or suspected breach: | |
| Date of actual or suspected breach: | |
| Date of discovery of actual or suspected breach: | |
| Date of internal notification of actual or suspected breach: | |

| **Preliminary assessment** | |
|---|---|
| Summary of the facts relating to the actual or suspected breach, including the types of personal data involved: | |
| Categories and approximate number of affected data subjects: | |
| Categories and approximate number of affected records: | |
| How sensitive is the personal data? | |
| Cause of the actual or suspected breach: | |
| Any other relevant information or comments: | |
| **Containment and recovery** | |
| Is the actual or suspected breach ongoing? | |
| What steps can be taken to contain the breach, i.e., to stop or minimize further loss, destruction or | |
| What steps can be taken to recover any lost personal data? | |
| Does the breach need to be reported to the police, for example if there is evidence of theft? | |
| Does any professional regulator or trade body need to be notified of the breach? | |
| Does the breach need to be reported to any relevant insurers, e.g. professional indemnity? | |
| **Detailed assessment** | |
| What types of personal data are involved, and does the breach involve any special categories of personal data | |
| Who is affected by the breach? | |
| What are the likely consequences of the breach for affected data subjects? | |

| | |
|---|---|
| Where personal data has been lost or stolen, are any protections in place such as encryption? | |
| What has happened to the personal data? | |
| What uses could a third party make of the personal data? | |
| Are there any other personal data breaches? | |
| Has the breach been recorded in the data breach register? | |
| Any other relevant information or comments: | |
| **Notifying the Supervisory Authorities** | |
| What is the type of breach? | |
| What is the nature of the personal data affected? | |
| What is the potential harm to data subjects? | |
| What is the sensitivity of the personal data affected? | |
| What is the volume of personal data affected? | |
| How easy is it to identify data subjects from the personal data? | |
| What is the number of affected data subjects? | |
| Any other relevant information or comments: | |
| Taking the above into account, is there a legal obligation to notify the Supervisory Authorities? | |
| **Notifying affected data subjects** | |
| Is there a legal or contractual obligation to notify affected data subjects? | |

| | |
|---|---|
| If there is no legal or contractual obligation, should affected data subjects be notified anyway? Consider | |
| What is the best way to notify affected data subjects? | |
| Do any data subjects, or categories of data subjects, need to be treated with care because of their special | |
| What additional information should be provided to data subjects about what they can do to limit the damage? | |
| How should affected data subjects contact the Company for further information or advice and how will | |
| How will we keep a record of who has been notified? | |
| Any other relevant information or comments: | |
| Is there any legal or contractual requirement to notify any other parties? | |
| **Response** | |
| What security measures were in place when the breach occurred? | |
| What further measures have been, or are to be, put in place to address the breach and mitigate its possible | |
| What further technical or organizational measures are to be put in place to prevent the breach happening | |
| Does further staff training on data protection awareness need to be conducted? | |
| Is it necessary to conduct a privacy risk assessment (DPIA)? | |
| Any other comments: | |
| **Approval of response plan** | |
| Name: Michael Hering | |
| Job title: Global Data Protection Officer | |
| Date: | |
| Signature: | |

# 4 APPENDIXES

## *4.1 Definition*

| Abbreviations | Description |
|---|---|
| PII, Personal Identifiable Information, Personal Data | Refer to the personal data defined by the EU GDPR (Article 4 (1)), 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| Data Subject | EU GDPR (Article 4 - 1),<br>Data subject refers to any individual person who can be identified, directly or indirectly. |
| Data Controller | EU GDPR (Article 4 - 7),<br>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),<br>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),<br>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),<br>A natural or legal person, public authority, agency or anybody other than the data subject, controller, processor and persons who under direct authority of controller or processor, are authorized to process personal data |
| DPO/GDPO | Data Protection Officer/Global Data Protection Officer |
| DPIA | Data Protection Impacted Assessment |
| PIMS | Personal Information Management System |
| EU | European Union |

### *4.2 Related Documents*

| No | Code | Name of documents |
|---|---|---|
| 1 | EU GDPR | EU General Data Protection Regulation |
| 2 | 95/46/EC | EU Data Protection Directive 95/46/EC |
| 3 | Privacy shield | EU-U.S. and Swiss-U.S. Privacy Shield Frameworks designed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce. |
| 4 | APPI | Act on the Protection of Personal Information, Japan. It came into force on 30 May 2017. |
| 5 | PDPA | Personal Data Protection Act 2012, Singapore |
| 6 | PDPO | Personal Data (Privacy) Ordinance, Hongkong, 2012 |
| 7 | PIPA | South Korea's substantial Personal Information Protection Act (PIPA) was enacted on Sept. 30, 2011 |
| 8 | PIPEDA | Personal Information Protection and Electronic Documents Act, Canada 2018 |
| 9 | Privacy Act, APPs, CDR | Privacy act Australia including Australian Privacy Principles, Consumer Data Right |
| 10 | HITRUST | Health Information Trust Alliance (CSF, Common Security Framework) |
| 11 | HIPAA | Health Insurance Portability and Accountability Act of 1996 (HIPAA), US |
| 12 | PCI DSS | Payment Card Industry Data Security Standard, May 2018 |
| 13 | CCPA | California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq. |
| 14 | VCDPA | Virginia Consumer Data Protection Act, 01/2023 |
| 15 | PDPL, UAE | Decree-Law No. 45 of 2021 |
| 16 | DPA Philippines | Republic Act 10173, Data privacy Act 2012 |
| 17 | PIPL | Personal Information Protection Law of the People's Republic of China and related laws and regulations |

| No | Code | Name of documents |
|---|---|---|
| 18 | PDPA Thailand | Thailand's Personal Data Protection Act, 06/2022 |
| 19 | PDPA Malaysia | Personal Data Protection Act 2010, Malaysia |
| 20 | TISAX | Trusted information security assessment exchange |
| 21 | BS10012: 2017 | British Standard Personal Information Management System |
| 22 | | Vietnamese laws on Privacy:<br>- Article 21 of the 2013 Constitution<br>- Article 38 of the Civil Code 2015<br>- Article 125 of the Penal Code<br>- Clause 2 of Article 19 of the Labor Code<br>Decree of the Vietnamese Government:<br>Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân<br>Came in force 07/2023 |
| 23 | FPT Software Personal Data Protection Handbook | PDP_ Handbook_Version_V3.4 |

### *4.3 Data Protection Law, Vietnam, Overview*

There is no single data protection law in Vietnam. Regulations on data protection and privacy can be found in various legal instruments. The right of privacy and right of reputation, dignity and honour and fundamental principles of such rights are currently provided for in Constitution 2013 ("**Constitution**") and Civil Code 2015 ("**Civil Code**") as inviolable and protected by law.

Regarding personal data, the guiding principles on collection, storage, use, process, disclosure or transfer of personal information are specified in the following main laws and documents:

- **Criminal Code** No. 100/2015/QH13, passed by the National Assembly on 27 November 2015
- Law No. 24/2018/QH14 on Cybersecurity, passed by the National Assembly on 12 June 2018 ("**Cybersecurity Law**");
- Law No. 86/2015/QH13 on Network Information Security, passed by the National Assembly on 19 November 2015; as amended by Law No. 35/2018/QH14 dated 20 November 2018, on amendments to some articles concerning planning of 37 Laws ("**Network Information Security Law**");
- Law No. 59/2010/QH12 on Protection of Consumers' Rights, passed by the National Assembly on 17 November 2010; as amended by Law No.35/2018/QH14 dated 20 November 2018, on amendments to some articles concerning planning of 37 Laws ("**CRPL**");
- Law No. 67/2006/QH11 on Information Technology, passed by the National Assembly on 29 June 2006; as amended by Law No. 21/2017/QH14 dated 14 November 2017 on planning ("**IT Law**");
- Law No. 51/2005/QH11 on E-transactions, passed by the National Assembly on 29 November 2005 ("**E-transactions Law**");
- Decree No. 85/2016/ND-CP dated 1 July 2016, on the security of information systems by classification ("**Decree 85**");
- Decree No. 72/2013/ND-CP dated 15 July 2013 of the Government, on management, provision and use of Internet services and online information; as amended by Decree No. 27/2018/ND-CP dated 1 March 2018 and Decree No.150/2018/ND-CP dated 7 November 2018 ("**Decree 72**");
- Decree No. 52/2013/ND-CP dated 16 May 2013 of the Government; as amended by Decree No. 08/2018/ND-CP dated 15 January 2018, on amendments to certain Decrees related to business conditions under state management of the Ministry of Industry and Trade and Decree No. 85/2021/ND-CP dated 25 September 2021 ("**Decree 52**");
- Decree No. 15/2020/ND-CP of the Government dated 3 February 2020 on penalties for administrative violations against regulations on postal services, telecommunications, radio frequencies, information technology and electronic transactions ("**Decree 15**");
- Circular No. 03/2017/TT-BTTTT of the Ministry of Information and Communications dated 24 April 2017 on guidelines for Decree 85 ("**Circular 03**");

- Circular No. 20/2017/TT-BTTTT dated 12 September 2017 of the Ministry of Information and Communications, providing for Regulations on coordinating and responding to information security incidents nationwide ("**Circular 20**");
- Circular No. 38/2016/TT-BTTTT dated 26 December 2016 of the Ministry of Information and Communications, detailing cross-border provision of public information ("**Circular 38**");
- Circular No. 24/2015/TT-BTTTT dated 18 August 2015 of the Ministry of Information and Communications, providing for the management and use of Internet resources, as amended by Circular No. 06/2019/TT-BTTTT dated 19 July 2019 ("**Circular 25**"); and
- Decision No. 05/2017/QD-TT 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.