Guideline

EXECUTION OF A DATA FLOW MAPPING UNDER PERSONAL DATA PROTECTION

Document Code	**08e-HD/SG/HDCV/FSOFT**
Version	**2.4**
Effective date	**01-Aug-2023**

TABLE OF CONTENT

1 INTRODUCTION 5

1.1 Purpose 5

1.2 Application Scope 5

1.3 Responsibility 6

2 DATA FLOW MAPPING 7

2.1 Key Elements 7

2.2 Type of Data 7

2.3 Data Flow Mapping 8

2.4 Data Workflow 8

2.5 Practical Steps 9

3 GUIDELINE CONTENT 10

3.1 Personal data inventory operation and data mapping timing 10

3.2 Summary and review of personal data inventory operations. 10

3.3 Data Retention 10

4 APPENDIXES 11

4.1 Definition 11

4.2 Related Documents 12

4.3 Data Protection Law, Vietnam, Overview 14

RECORD OF CHANGE

No	Effective Date	Version	Change Description	Reason	Reviewer	Final Reviewer	Approver
1	21-Oct-2019	1.0	Newly issued	Legal requirement	TrangNN4	Michael Hering	HoanNK
2	11-May-2020	1.1	Add sub-section: Summary and review of personal data inventory operations Update section GUIDELINE CONTENT, INTRODUCTION	Update according to Annually revision requirement	TrangNN4	Michael Hering	HoanNK
3	01-Jul-2020	1.1.1	HITRUST	HITRUST requirement	TrangNN4	Michael Hering	HoanNK
4	19-Oct-2020	1.2	Update sections: related document, guideline content	Legal requirement	TrangNN4	Michael Hering	HoanNK
5	01-May-2021	2.0	Change the document structure. Update sections: Practical Steps, Guideline Content, Related Document Add Responsibility section	Legal requirement	TrangNN4	Michael Hering	HoanNK
5	01-Oct-2021	2.1	1.2 added: statement_PIMS scope_V1.0, 1.3 added: Guideline_Personal Data Retention_v3.1, Procedure_Retention of Records_V1.0, 4.2 added: statement_PIMS scope_V1.0, Guideline_Personal Data Retention_v3.1, Procedure_Retention of Records_V1.0	Legal requirement	TrangNN4	Michael Hering	HoanNK
6	01-Apr-2022	2.2	4.2 14 added: PDPL, UAR, Decree-Law No. 45 of 2021 4.2 16 added: Decree of the Vietnamese Government: Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân 4.2 17 PDP_ Handbook_Version_V3.2 4.2 18 added: 15e-HD/SG/HDCV/FSOFT 4.2 19 added: 11e-QT/SG/HDCV/FSOFT 4.2 20: 05e-HD/SG/HDCV/FSOFT				
7	01-Nov-2022	2.3	Added 4.3. Data Protection Law, Vietnam, Overview. Added 4.2 15 Republic Act 10173 Data privacy Act 2012 Added 4.2 17 Personal Data Protection Act 2010, Malaysia Added 3.2 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 4.2 14, 18 changed 4.2 22: Came in force 07/2023 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 and templates set a globally applicable data protection and security standard for FPT Software and regulates the sharing of information between FPT Software, subsidiaries, and legal entities. FPT Software have established guiding data protection principles – among them transparency, data economy and data security – as FPT Software guidelines.

The GDPR and other national/international laws/regulations extends the rights of individuals, and requires FPT Software to implement appropriate technical measures, as well as clear policies, procedures, guidelines, processes, and other organizational measures to protect personal data.

1.1 Purpose

Data flow mapping is a key step to ensure compliance with the GDPR or other national/international laws/regulations. Organizations often process much more data than they realize, and data flow maps help them to identify the data they are holding and where it is moving.

Walk through the information lifecycle to identify unforeseen or unintended uses of data is scope of data flow mapping. Doing it helps to eliminate unnecessary data transfers and ensures that employees are aware of the practical implications of data usage. Tracking the interaction points between the parties involved – both internal and external – ensures that all uses of the data can be identified.

Also, future uses of data need to be properly thought out, even if FPT Software has no immediate plans. By predicting how data will be used in months or years to come, we can make sure that appropriate resources and security measures are in place and give data subjects advanced notice.

1.2 Application Scope

See Policy_PIMS scope_V1.3.

This guideline is binding for all departments and functions globally which are involved in personal identifiable information processing.

1.3 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). The GDPO is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements and other 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 to execute or guide all data flow mapping activities. GDPO shall document and archive the data flow mapping.

More details in Guideline_Personal Data Protection Organization_V3.4. For retention see Procedure_Retention of Records_V1.3 and Guideline_Personal Data Retention_v3.4.

2 DATA FLOW MAPPING

2.1 Key Elements

A data flow map should identify:

- Data items
- Formats
- Transfer methods
- Locations

These elements need to be established because each can introduce different risks to the data. The data items are the details of the information itself, i.e., a person's name, email, address, etc.

The format of the data refers to the methods by which the data is collected, stored, processed, and released. It is obtained as a hard copy (paper records), via a form on a website, harvested from emails, or some other method.

FPT Software then needs to look at how the data is being transferred – it is by post, telephone, secured connection or social media, and is the transfer internal or external.

FPT Software will also need to look into the location of the data and where it is stored. This could be in an office, in the Cloud, with a third party, and so on.

GDPO should work with OB and FSU team members to discuss what happens at each stage of the data collection process, clarifying where the data goes and who sees it.

2.2 Type of Data

The first challenges are to determine what personal data is being collected. There are many different types of personal data, such as names, ID numbers, passport numbers, IP addresses, usernames, medical records, biometric data, smart meter number, number plat and so on. Any such information will be subject to the GDPR or other national/international laws/regulations if it relates to an identifiable, living person.

FPT Software must also identify the source of the data and the circumstances under which they are collecting it. What kinds of technical and organizational safeguards are in place to protect the rights and freedoms of the data subjects? The GDPR and other national and international laws are, after all, about protecting individuals, not the entity that collects the data. FPT Software needs to understand its legal and regulatory obligations, and ensure it meets those obligations.

2.3 Data Flow Mapping

There are several ways to gather information about processing operations.

Information can be collected by inspecting existing documents, running workshops, conducting questionnaires or observing business activities. If there is no documented workflow describing how personal data is collected and processed, it is worthwhile to send out a team to investigate (data inventory).

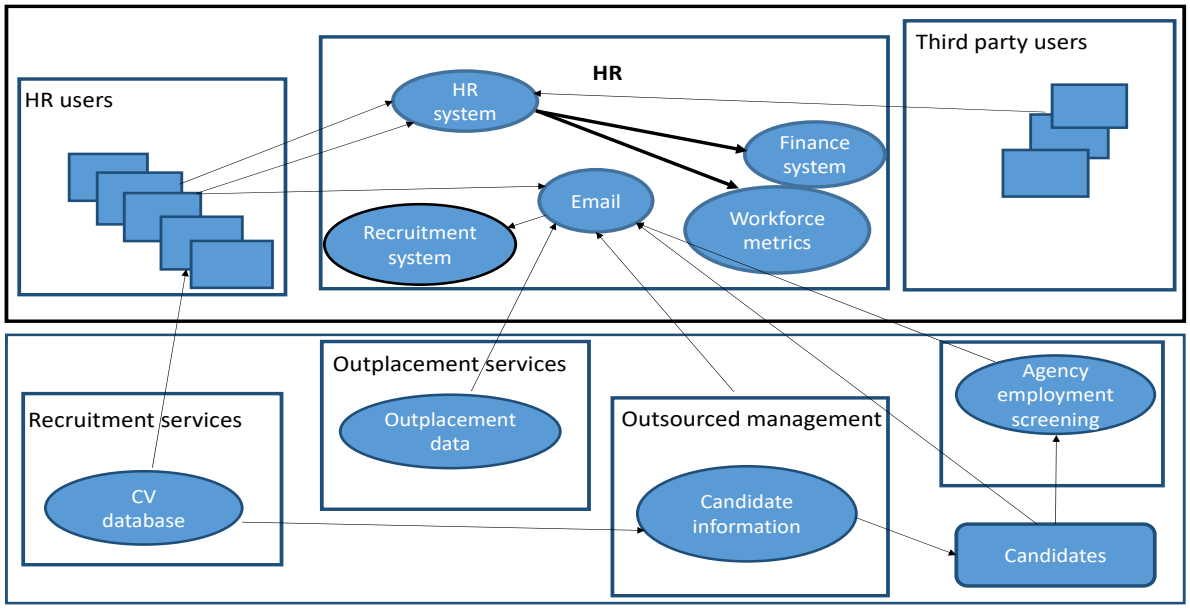
With delivery teams it must be discussed what happens at each stage of the data collection process, clarifying where the data goes and who sees it. What are the retention periods? Where the data are stored. How are the data protected? Templates, including data flow mapping applications, could help with these discussions and ultimately map data.

2.4 Data Workflow

A workflow has data coming in one end and going out the other, with some process happening to the data in between. In many cases, the output of a process or a workflow provides the input for another.

Understanding workflows requires you to understand the personal data and the form it has been collected in. We must look at how the data was captured, who is accountable for it, where it is located and who has access to it. We must establish if the information has been disclosed/shared with anyone, and if the workflow interfaces with or transfers information to any other processes.

Below an example of a less structured data flow, looking at how CVs might be processed in a recruitment campaign or as part of a company recruitment process. This data flow shows the different ways in which the data is coming in, the number of people who will use the data and where the data is going. An organization must be able to track each of these movements in order to put the appropriate checks in place, such as controls managing transfers to third parties involved in the process. Ensuring these measures are appropriate to privacy and other related risks is an essential part of GDPR compliance and other national/international laws/regulations.



2.5 Practical Steps

Gathering the necessary information to populate data flow maps is critical. A data flow audit can be used to gather this information and construct data flow maps.

2.5.1 Documentation of Processing

The first step is to document the scope and purposes of processing. It is not possible to work out the impact on the rights and freedoms of natural persons unless knowing what data are collected and where it is flowing. If we are not sure how to handle personal data, we cannot provide assurances that data protection is fundamental to how we operate.
By running data flow audits, we also build a personal data inventory (Guideline_Personal_Data_Inventory_Management_V3.4).
If we are not aware of all the data of our company possesses, we cannot reliably accommodate data subject access requests, in contravention of the GDPR and other national/international laws/regulations.

When building a personal data inventory, we need to establish the data items, data subject and the lawful basis for processing.

2.5.2 Mapping and Inventory

The next step is to enter this information into a data map. This will provide a visual depiction of the data we hold, how it moves through our organization and where it is processed.

2.5.3 Including related Assets

Step three is to add the supporting assets used to process personal data. These include any location where data is stored or used, such as an app or a report file, as well as processes that involve personal data, such as secure destruction.

Assets form part of the control environment – for instance, if personal data is managed by a device that uses an unpatched operating system, a range of vulnerabilities are introduced that must be dealt with as part of the FPT Software's risk management activities.

2.5.4 Data Transfers

Step four is to add data transfers to the map to show the flow of data between assets, so that we can make sure there are no intermediate steps. It also enables us to consider security in the data flows, both when the data is in transit and when it is at rest.

2.5.5 Process review

The final step is to review the process to ensure there is nothing we have missed. The outputs of the data mapping will help us to meet the obligations under the GDPR and other national/international laws/regulations, so it is essential that the results are thorough. In particular, this will help FPT Software to develop a record of processing activities (Article 30 of the GDPR) and identify activities that may need to be reviewed with a data protection impact assessment (DPIA) (Guideline_Risk_Management_DPIA_V2.4).

3 GUIDELINE CONTENT

3.1 Personal data inventory operation and data mapping timing

Every year every FPT Software department, unit, legal entity, or subsidiary is obligated to perform a personal data inventory and where reasonable a mapping.

After every change of the organizational structure or business process of a department, unit, legal entity or subsidiary, the department, unit, legal entity, or subsidiary is obligated to perform a personal data inventory.

In case of a personal data inventory, the department, unit, legal entity or subsidiary must use, and fill the “Template_Personal Data Processing Inventory_V2.6”.

3.2 Summary and review of personal data inventory operations.

The Data Protection Office (FHO.LRC) supports the units with a data inventory interview/audit.

The execution and completion of personal data inventory is the responsibility of the department Data Protection Representative based on the advice of the GDPO. The personal data inventory should be reviewed by the head of relevant department unit, legal entity or subsidiary and then approved by the GDPO.

After the assessment of risk management group is completed, the GDPO must review it. GDPO has develop a final privacy impact analysis and risk mitigation plan. The GDPO must bring the results and the mitigation plan to the attention of the FPT Software Board Member responsible for data protection.

3.3 Data Retention

The records of the personal data inventory, the results of the risk assessment shall be kept in accordance with the Guideline_Personal Data Retention_V3.4 and Guideline_Personal Data Protection Policy Development_v2.4.

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), Data subject refers to any individual person who can be identified, directly or indirectly.
Data Controller	EU GDPR (Article 4 - 7), Data Controller means the natural or legal person, public authority, agency or anybody which alone or jointly with others, determines the purpose and means of processing of personal data; where the purpose and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Data Processor	EU GDPR (Article 4 - 8), Data Processor means a natural or legal person, public authority, agency or anybody which processes data on behalf of the controller.
Recipient	EU GDPR (Article 4 - 9), A natural or legal person, public authority, agency or anybody, to which the personal data are disclosed, whether third party or not.
Third Party	EU GDPR (Article 4 - 10), A natural or legal person, public authority, agency or anybody other than the data subject, controller, processor and persons who under direct authority of controller or processor, are authorized to process personal data
DPO/GDPO	Data Protection Officer/Global Data Protection Officer
DPIA	Data Protection Impacted Assessment
PIMS	Personal Information Management System
EU	European Union

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: - 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

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-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.