Guideline

COMPLAINTS AND APPEALS HANDLING, DATA SUBJECT RIGHTS EXERCISE

Document Code	03e-HD/SG/HDCV/FSOFT
Version	3.5
Effective date	01-Dec-2024

TABLE OF CONTENT

RECORD OF CHANGE

No	Effective Date	Version	Change Description	Reason	Reviewer Local DPO VN	Final Reviewer GDPO	Approver
1	10-May-2019	1.0	Newly issued	Business requirement	Minh	Michael Hering	CFO/COO
2	21-Oct-2019	1.1	Revision	Legal requirement	Trang	Michael Hering	CFO/COO
3	11-May-2020	2.1	Add sub-section: Application of national Laws and Governance-Change title and content of following sections: + 2.3. Processing into Types of Complaints and Appeals + 2.4. Reply into Complaints Procedure has four levels of handling and escalation + 2.5. Record into Data Protection Complaint Inventory-Update Introduction and guideline content.	Update according to annually revision requirement	Trang	Michael Hering	CFO/COO
4	01-Jul-2020	2.1.1	HITRUST	HITRUST requirement	Trang	Michael Hering	CFO/COO
5	19-Oct-2020	2.2	Update section: related document Change “Data Breach Contact List Q1_2020” into “Data Breach Contact List Q4_2020”	Legal requirement	Trang	Michael Hering	CFO/COO
6	01-May-2021	3.0	- Change the document structure, - Update more information for the Responsibilities/ Governance section.	Legal requirement	Trang	Michael Hering	CFO/COO
7	01-Oct-2021	3.1	1.2 add: statement_PIMS scope_V1.0, 3.2 add: Record_internal contracts_V1.0 Record_DP contacts_V1.0 Record_authorities_Key-Supplier_V1.0	Legal requirement	Trang	Michael Hering	CFO/COO
8	01-Apr-2022	3.2	1.2 added: Policy_PIMS scope_V1.1 2.2 added: Guideline_Data Breach Incident Response_v3.2, Procedure_Personal Data Breach Notification_V1.1) 3.2 14 added PIPL, 3.2 15 added: PDPL, UAR, Decree-Law No. 45 of 2021 3.2 17 added: Decree of the Vietnamese Government:	Biannually revision	Linh Do Thi Dieu	Michael Hering	CFO/COO

No	Effective Date	Version	Change Description	Reason	Reviewer Local DPO VN	Final Reviewer GDPO	Approver
			Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân 3.2 18 PDP_ Handbook_Version_V3.2 3.2 19: 01e-DM/SG/HDCV/FSOFT				
9	01-Nov-2022	3.3	Deleted 2.5 until 30.09.2021 then DPO Tool, WEB application for handling, incidents Added 3.3. Data Protection Law, Vietnam, Overview. Added 3.2 15 Republic Act 10173 Data privacy Act 2012 Added 3.2 17 PDPA Added 3.2 18 TISAX	Biannually revision	Linh Do Thi Dieu	Michael Hering	CFO/COO
10	01-Aug-2023	3.4	Adjust document version numbers added 3.2 14, 18 changed 3.2 22: Came in force 07/2023 changed 3.3 PDPD was finalized and was coming in force 07/2023	Biannually revision	Linh Do Thi Dieu	Michael Hering	CFO/COO
11	14-May-2024	3.4.1	change document classification, deleted for 'internal use'	Document classification	Linh Do Thi Dieu	Michael Hering	CFO/COO
12	01-Dec-2024	3.5	1. Added PDPD13, Added 3.20, 3.24 Changed 3 7 to March 15, 2024	Biannually revision	Linh Do Thi Dieu	Michael Hering	CFO/COO

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, PDPD13 VN 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.

1.1 Purpose

The purpose of this guideline is to outline the internal personal data processing complaint and appeal handling procedure of FPT Software, and our internal and external response procedure. It should be read in conjunction with our data protection policy Policy_Personal Data Protection Management_v3.5.

Description of personal data processing complaint/appeal 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).

In order to enable the parties to complain about the personal data processing in a structured way and that complaints can be handled promptly and correctly; the company established these guidelines in accordance with the requirements of personal data protection related laws and regulations.

1.2 Application Scope

See Policy_PIMS scope_V1.4.

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

A thorough and transparent complaints procedure is considered necessary to enable the FPT Software to consider what happened and how to rectify errors in relation to breaches of Personal Data Protection and Data Subject right. This guideline follows FPT Software Corporate Data Protection Policy. This Data Protection Complaints Guideline ensures that all complaints are treated with due consideration, fairness, and equitability.

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.

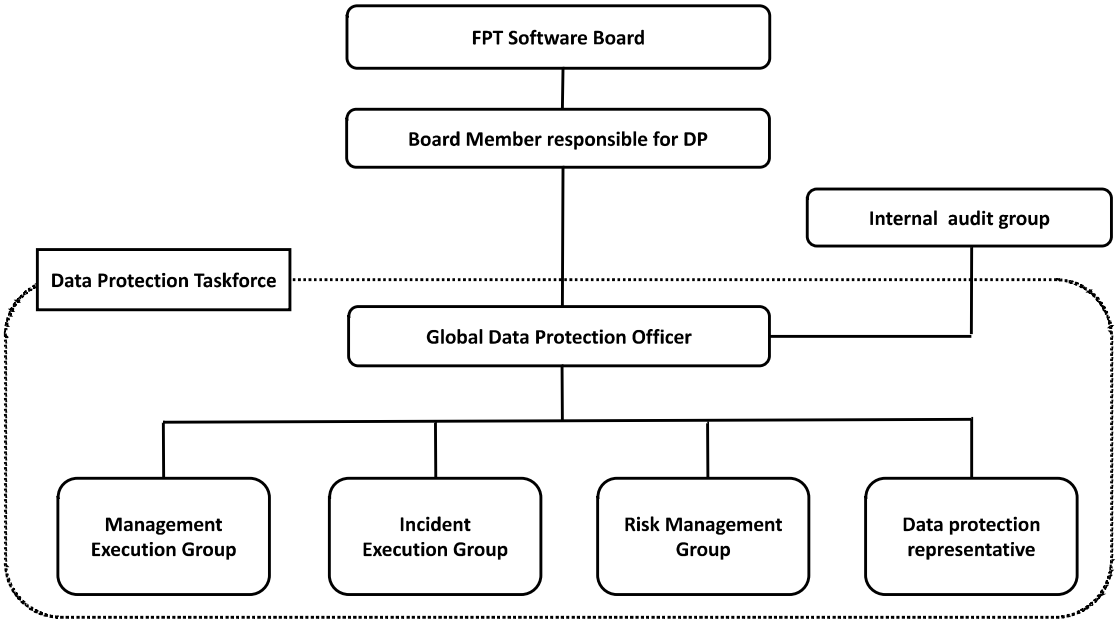
Each subsidiary or legal entity of FPT Software is responsible for compliance with the Data Protection Policy, this guideline and the legal obligations. If there is reason to believe that legal obligations contradict the duties under the Data Protection Policy or the guidelines, the relevant subsidiary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

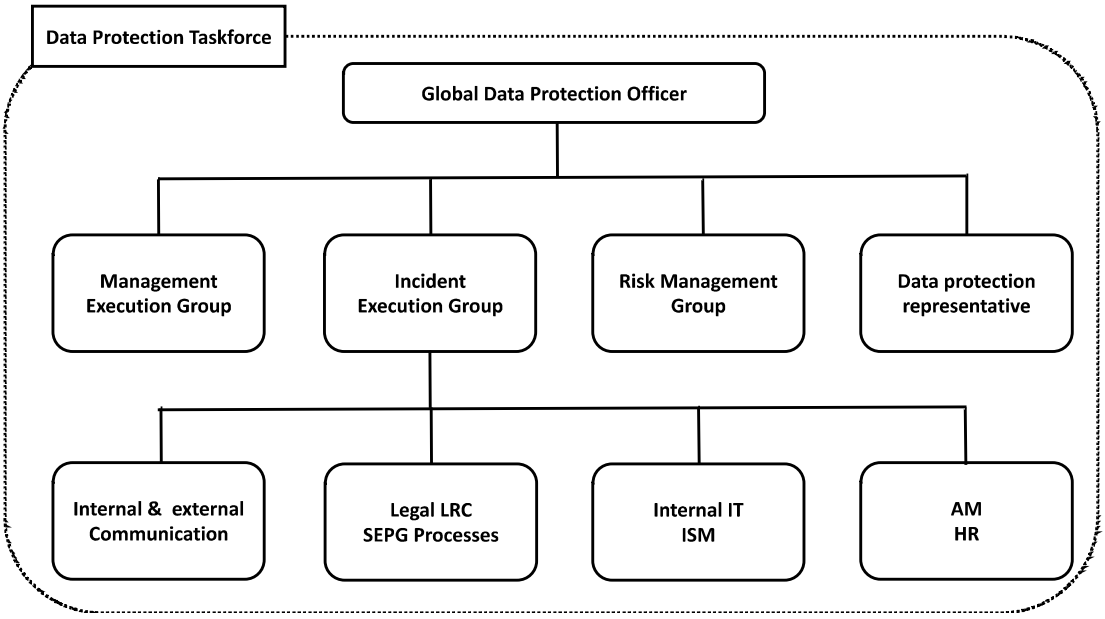
1.4 Responsibilities/Governance

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 supervises the processing and response to Data Subjects regarding personal information complaints and appeals. GDPO must ensure that all departments of the company are following the company guidelines and the respective laws.





Acceptance Window

Accept complaints and appeals

Confirm the identity of the applicant

Report to Incident Execution Group the reason, processing and result of complaints and appeals

Incident Execution Group

Assist the departments and individuals to manage, to respond and to solve complaints and appeals

Track the complaints and appeals handling process

More details in Guideline_Personal Data Protection Organization_v3.5.

2 GUIDELINE CONTENT

If anyone wishes to complain to FPT Software about how their personal data has been processed, their personal data processing complaint has been handled, or appeal against any decision made following a complaint, they can submit their complaint in writing. This should be addressed directly to the Global Data Protection Office of FPT Software. The contact information is on the FPT Software Web presence (home page).

The company's customer service department or account manager is the acceptance window for complaints and appeals from customers, HR department is acceptance window for complaints and appeals from FPT Software employees. The Incident Execution Group is the reply window.

If complaints regarding how personal data has been processed submitted to FPT Software GDPO, customer service department or HR department, a receipt will be acknowledged within 7 working days. Incident Execution Group will review and respond in writing to a complaint within 14 working days of receipt of the complaint. If a longer time is required Incident Execution Group will notify the Complainant of the delay and will provide an estimate of when he will provide a substantive response. If a Complainant is dissatisfied with the way in which their complaint has been handled, then they can forward their complaint to FPT Software GDPO.

2.1 Acceptance

Entry of complaints and appeals according to the company regulations by

- Mail in writing
- Personal visits
- phone call
- By-mail

After accepting complaints and appeals, the acceptance window should be processed in accordance with the procedures. The relevant contact information of the applicant for subsequent processing and replying actions has to be recorded and verified.

2.2 Verify and acceptance request

After accepting the applicant's complaint and appeal application, it shall be submitted to the responsible supervisor for review and approval in accordance with the procedures of the company, the Incident Execution Group will take over the responsibility for further actions and the GDPO shall be informed without any delay.

If the content of the appeal relates to exercise rights of the data subject, it shall be processed in in the same way (same process) as an appeal or complaint.

If the content of the appeal relates to a personal data leak or abuses, it shall be processed in accordance with the provisions of Personal Data Incident Management Process (Guideline_Data Breach Incident Response_v3.5, Procedure_Personal Data Breach Notification_v1.4).

2.3 Types of Complaints and Appeals

Informal Complaint

The Complainant makes a verbal complaint to an FPT Software employee or Representative who then logs and reports it immediately to the line manager and the GDPO. GDPO decides whether it is a level 1 or level 2 process that is best required in all the circumstances.

The Incident Execution Group check the complaint, undertakes any required investigation into the circumstances of the allegation, agrees resolution with the Complainant and implements solution.

The Complainant confirms in writing that they are satisfied with the resolution.

Timeframe: Immediate to within 14 working days.

Formal Compliant

The complaint is received either verbally, in writing by email, phone, website or by personal submission. The complaint is logged and reported to the DPO to deal with and action. GDPO decides the level of process that is best required in all the circumstances. The Receipt of the complaint is acknowledged within one working day.

The Complainant will receive a response from the GDPO within 14 working days.

The Incident Execution Group check the complaint, undertakes any required investigation into the circumstances of the allegation, agrees resolution with the Complainant and implements solution.

The Complainant confirms in writing that they are satisfied with the resolution.

If applicable, the results of the investigation into the matter shall be shared with the Supervisory Authorities and FPT Software shall liaise with the Supervisory Authorities if and as required.

Timeframe: Between one working day and, at the latest, 21 working days after submission of complaint.

Anonymous Complaints

Complaints submitted anonymously will be considered if there is enough information in the complaint to enable FPT Software to make further enquiries. If, however, an anonymous complaint does not provide enough information to enable FPT Software to take further action it may decide not to pursue it further. However, FPT Software may give consideration to the issues raised, and will record the complaint so that corrective action can be taken as appropriate. Any decision not to pursue an anonymous complaint must be authorized by the GDPO who is responsible for dealing with Data Protection breaches.

2.4 Complaints Procedure has four levels of handling and escalation

Level 1

Informal Complaints – delegation by the Incident Execution Group to a suitable person or team knowledgeable about the circumstances for their investigation, discussion and resolution with the Complainant.

Level 2

Formal Complaints – investigation, discussion and resolution with the Complainant by the Incident Execution Group. GDPO must be informed about at every time and must approve the final resolution.

Level 3

Escalation to the GDPO – consideration of the complaint and the prior investigation, communication and efforts to resolve.

Level 4

Final escalation to the DP responsible board member (CFO).

All complaints should go fully through level 1 or 2 before/if they proceed any further to level 3. The GDPO can decide, on behalf of FPT Software, that a complaint is vexatious or of no merit to justify level 4 and can refuse any Complainant's request for a level 4 review. Such a decision is to be undertaken in the knowledge that the Complainant's next step would be to the Supervisory Authorities or legal action which are factors that shall be taken into account in such decision.

Any Level 2 Formal Complaint that is reasonably established to have been a reportable breach of Data Protection laws or regulations shall be reported to the Supervisory Authorities as soon as reasonably possible after it has been established, and within 72 hours.

Receipt of the escalated complaint is acknowledged within one working day.

The DPO fully briefs DP responsible board member (CFO) hearing the complaint concerning its history and the details and conclusions of any prior Level 1 or Level 2 investigations. Within 5 working days, the Complainant is advised of when the relevant DP responsible board member (CFO) will be considering the complaint which will be no more than 2 working weeks from the date of the acknowledgement of the escalated complaint.

The Complainant will be invited to make a final written submission to the DP responsible board member (CFO). If the Complainant is asked to attend a meeting in person, the Complainant may be accompanied by an independent person for the purposes of support. The DP responsible board member (CFO) concerned will proceed with review of the substance of the case and its handling.
The Complainant will receive a response from the DP responsible board member (CFO) or the DPO within 10 working days after the DP responsible board member's (CFO) consideration of the complaint. The DP responsible board member (CFO)'s decision is final, subject to any ruling or information relating thereto from the Supervisory Authorities. Timeframe: Between one working day and, at the latest, 28 working days after submission of complaint.

Method: Written response from the DP responsible board member (CFO) or on his behalf by the DPO.

2.5 Data Protection Complaint Inventory

FPT Software shall keep a written log of complaints received and actions taken, and decisions reached in a Data Protection Complaint Inventory. This shall consist of an adequate record to be retained of a case, any reporting to any Supervisory Authorities, action taken by FPT Software and action/conclusion required by any Supervisory Authorities (Template_Data Subject Request Incident Compliant Appeal Register_v1.5, DS requests, complaints and appeals).

3 APPENDIX

3.1 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

3.2 Related Documents

No	Code	Name of documents
1	EU GDPR/GDPR UK	EU General Data Protection Regulation/UK
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 March 15, 2024
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	PDPL Indonesia	Data protection in Indonesia is regulated by Law No. 27 of 2022 on Personal Data Protection (“PDP Law”)
19	PDPA Thailand	Thailand’s Personal Data Protection Act, 06/2022
20	PDPA Malaysia	Personal Data Protection Act 2010, Malaysia
21	TISAX	Trusted information security assessment exchange
22	BS10012: 2017	British Standard Personal Information Management System
23	ISO 27001	Information security, cybersecurity and privacy protection — Information security management systems
24	ISO 27701	ISO/IEC 27701:2019 (formerly known as ISO/IEC 27552 during the drafting period) is a privacy extension to ISO/IEC 27001. The design goal is to enhance the existing Information Security Management System (ISMS) with additional requirements in order to establish, implement, maintain, and continually improve a Privacy Information Management System (PIMS). The standard outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage privacy controls to reduce the risk to the privacy rights of individuals.
25	PDPD13, VN	Decree of the Vietnamese Government: PDPD13 Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân 07/2023
26	FPT Software Personal Data Protection Handbook	PDP_ Handbook_Version_V3.5

3.3 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.