Guideline

RISK MANAGEMENT DPIA

Document Code	**10e-HD/SG/HDCV/FSOFT**
Version	**2.4**
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	Legal requirement	TrangNN4	Michael Hering	HoanNK
2	11-May-2020	1.2	-Change document name: "GDPR DPIA" into "Risk Management DPIA" Add the content of Introduction section -Update 1.1. Purpose, 1.2. Application Scope, -Add more related documents	Legal requirement	TrangNN4	Michael Hering	HoanNK
3	01-Jul-2020	1.2.1	HITRUST	HITRUST requirement	TrangNN4	Michael Hering	HoanNK
4	19-Oct-2020	1.3	Update related document section and update related document name at Guideline content section	Legal requirement	TrangNN4	Michael Hering	HoanNK
5	01-May-2021	2.0	Change the document structure. Update sections:DPIA Definition, DPIA, Responsibilities, Related Documents.	Legal requirement	TrangNN4	Michael Hering	HoanNK
6	01-Oct-2021	2.1	1.2 added: statement_PIMS scope_V1.0, 2.1 added: template_DPIA_compact_V1.0, 3.1 added: template_DPIA_compact_V1.0, 5.2 added: statement_PIMS scope_V1.0., template_DPIA_compact_V1.0	Legal requirement	TrangNN4	Michael Hering	HoanNK
7	01-Apr-2022	2.2	1.2 added: Policy_PIMS scope_V1.1 1.4 changed to: General responsibility 1.4 added: Execute DPIA where appropriate 3.1 added: 32e-BM/SG/HDCV/FSOFT 5.2 13 added PIPL, 5.2 14 added: PDPL, UAR, Decree-Law No. 45 of 2021 5.2 16 added: Decree of the Vietnamese Government: Nghị Định Quy Định Về Bảo Vệ Dữ Liệu Cá Nhân 5.2 17 PDP_ Handbook_Version_V3.2 5.2 19: 19e-BM/SG/HDCV/FSOFT 5.2 20: 32e-BM/SG/HDCV/FSOFT	Biannually revision	LinhDTD1	Michael Hering	HoanNK

No	Effective Date	Version	Change Description	Reason	Reviewer	Final Reviewer	Approver
			5.2 21: 15e-HD/SG/HDCV/FSOFT				
8	01-Nov-2022	2.3	Added 5.3. Data Protection Law, Vietnam, Overview. Added 5.2 15 Republic Act 10173 Data privacy Act 2012 Added 5.2 17 PDPA Added 5.2 18 TISAX	Biannually revision	LinhDTD1	Michael Hering	HoanNK
9	01-Aug-2023	2.4	Adjust document version numbers added 5.2 14, 18 changed 5.2 22: Came in force 07/2023 changed 5.3 PDPD was finalized and was coming in force 07/2023	Biannually revision	LinhDTD1	Michael Hering	HoanNK

1 INTRODUCTION

FPT Software Company, Ltd. Corporate Data Protection Policy, guidelines, procedures, 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.

1.1 Purpose

A data protection impact assessment (DPIA) is a process helping to minimize the data protection risks of a project.

DPIA is mandatory for certain types of processing, or any other processing that is likely to result in a high risk to individuals. It is also recommended to do a DPIA for any other major project which requires the processing of personal data.

DPIA must:

- Describe the nature, scope, context, and purposes of the processing
- Assess necessity, proportionality, and compliance measures
- Identify and assess risks to individuals
- Identify any additional measures to mitigate those risks.

To assess the level of risk, both the likelihood and the severity of any impact on individuals must be considered. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

The Global Data Protection Officer must be consulted and, where appropriate, individuals and relevant experts. If a high risk is identified that cannot be mitigate, the EU Supervisory Authority must be consulted before starting the processing.

The Supervisory Authority will give written advice within eight weeks, or 14 weeks in complex cases.

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

1.2 Application Scope

See Policy_PIMS scope_V1.3.

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

1.3 Application of national Laws

This Data Protection Policy, guidelines and templates comprises the internationally accepted data privacy principles without replacing the existing national laws. It supplements the national data privacy laws. The relevant national law will take precedence in the event that it conflicts with the Data Protection Policy and guidelines, or it has stricter requirements than this Policy and guidelines. The content of the Data Protection Policy and guidelines must also be observed in the absence of corresponding national legislation. The reporting requirements for data processing under national laws must be observed.

Each subsidiary or legal entity of FPT Software is responsible for compliance with the Data Protection Policy, this guideline, and the legal obligations. If there is reason to believe that legal obligations contradict the duties under the Data Protection Policy or the guidelines, the relevant subsidiary or legal entity must inform the Global Data Protection Officer. In the event of conflicts between national legislation, the Data Protection Policy, and this guideline, FPT Software Global Data Protection Officer will work with the relevant subsidiary or legal entity of FPT Software to find a practical solution that meets the purpose of the Data Protection Policy and this guideline.

1.4 Responsibility

FPT Software Board Member responsible for DP	:	General responsibility
Risk Management Group	:	Consultation of FPT Software Units regarding DPIA
Global Data Protection Officer	:	Consultation of FPT Software Units regarding DPIA, Execute DPIA where appropriate Review/approve DPIA results and risk mitigation measures Communication with EU Supervisory Authority or other Data Protection Supervisory Authorities depending on country and local law requirements

2 GUIDELINE CONTENT

2.1 DPIA Definition

A DPIA is a way to analyze personal data processing and helps to identify and minimize data protection risks systematically and comprehensively.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm –- to individuals or to society at large, whether it is physical, material, or non- material.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals.

A DPIA does not have to eradicate the risks altogether but should help to minimize risks and assess whether or not remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations. It's important to embed DPIAs into our organizational processes. A DPIA is not a one-off exercise and should be seen as an ongoing process, and regularly review.

DPIAs are designed to be a flexible and scalable tool that apply to a wide range of sectors and projects. Conducting a DPIA does not have to be complex or time-consuming in every case, but there must be a level of rigor in proportion to the privacy risks arising.

Template_Risk Management DPIA_v3.4 or Template_DPIA Compact_v1.3 should be used.

2.2 Benefits from DPIA

DPIAs are an essential part of our accountability obligations. Conducting a DPIA is a legal requirement for any type of processing that is likely to result in high risk. Failing to carry out a DPIA in these cases may lead to enforcement action, including a fine of up to €10 million, or 2% global annual turnover if higher.

A DPIA also brings broader compliance benefits, as it can be an effective way to assess and demonstrate our compliance with all data protection principles and obligations.

DPIAs are not just a compliance exercise. An effective DPIA allows to identify and fix problems at an early stage, bringing broader benefits for both individuals and the processing organization.

It can reassure individuals that their interests are protected and negative impact on them is reduced as much as possible. Conducting and publishing a DPIA can also improve transparency and make it easier for individuals to understand how and why their personal data are processed.

In turn, this can create potential benefits for company's reputation and relationships with individuals.

There can also be financial benefits. Identifying a problem early on generally means a simpler and less costly solution, as well as avoiding potential reputational damage later on. A DPIA can also reduce the ongoing costs of a project by minimizing the amount of information be collect where possible and devising more straightforward processes for staff.

In general, consistent use of DPIAs increases the awareness of privacy and data protection issues within the organization and ensures that all relevant staff involved in designing projects think about privacy at the early stages and adopt a 'data protection by design' approach.

2.3 Use of DPIAs

A DPIA can cover a single processing operation, or a group of similar processing operations. It can be possible to rely on an existing DPIA if it covered a similar processing operation with similar risks.

DPIA can be used effectively throughout the development and implementation of a project or proposal, embedded into existing project management or other organizational processes.

For new projects, DPIAs are a vital part of data protection by design. They build in data protection compliance at an early stage, when there is most scope for influencing how the proposal is developed and implemented.

It is important to remember that DPIAs are also relevant if changes to an existing system are planned. In this case it has to be ensured that a DPIA is performed at a point when there is a realistic opportunity to influence those plans.

Recital 84 of the GDPR:

"the outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation."

DPIA is not simply a rubber stamp or a technicality as part of a sign-off process. It's vital to integrate the outcomes of DPIA back into the project plan.

DPIA should not be seen as a one-off exercise to file away. A DPIA is a 'living' process helping to manage and to review the risks of the processing and measures put in place on an ongoing basis. It must be kept under review and reassess if anything changes.

In particular, if there are any significant changes to how or why of the processing of personal data, or to the amount of data be collected, it needs to be checked that DPIA assesses any new risks. An external change to the wider context of the processing should also be prompted to review DPIA. For example, if a new security flaw is identified, new technology is made available, or a new public concern is raised over the type of processing or the vulnerability of a particular group of data subjects.

2.4 Types of Risks

There is no explicit definition of 'risk' in the GDPR, but the various provisions on DPIAs make clear that this is about the risks to individuals' interests. Article 35 says that a DPIA must consider "risks to the rights and freedoms of natural persons". This includes risks to privacy and data protection rights, but also effects on other fundamental rights and interests.

The key provision here is Recital 75, which links risk to the concept of potential harm or damage to individuals:

"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymization, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data...".

The focus is therefore on any potential harm to individuals. The risk-based approach is not just about actual damage and should also look at the possibility for more intangible harm. It includes any "significant economic or social disadvantage". The impact on society as a whole may also be a relevant risk factor.

A DPIA must assess the level of risk, and in particular whether it is 'high risk'. The GDPR is clear that assessing the level of risk involves looking at both the likelihood and the severity of the potential harm.

2.5 Reasons for DPIA

Article 35(1) says a DPIA must be performed where a type of processing is likely to result in a high risk to the rights and freedoms of individuals:

"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."

Risk in this context is about the potential for any significant physical, material or non-material harm to individuals.

To assess whether something is 'high risk', the GDPR is clear that it needs to be considered both the likelihood and severity of any potential harm to individuals. 'Risk' implies a more than remote chance of some harm. 'High risk' implies a higher threshold, either because the harm is more likely, or because the potential harm is more severe, or a combination of the two. Assessing the likelihood of risk in that sense is part of the job of a DPIA.

GDPR doesn't define 'likely to result in high risk'. The important point here is not whether the processing is actually high risk or likely to result in harm – that is the job of the DPIA itself to assess in detail. Instead, the question is a more high-level screening test: are there features which point to the potential for high

risk? Screening for any red flags which indicate that a DPIA needs to be performed to look at the risk (including the likelihood and severity of potential harm) in more detail.

Article 35(3) lists three examples of types of processing that automatically requires a DPIA. This does not mean that these types of processing are always high risk or are always likely to cause harm – just that there is a reasonable chance they may be high risk and so a DPIA is required to assess the level of risk in more detail.

2.6 Types of Processing automatically require a DPIA

Article 35(3) lists three examples of types of processing that automatically requires a DPIA.

Systematic and extensive profiling with significant effects:

"(a) any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person".

Large scale use of sensitive data:

"(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10".

Public monitoring:

"(c) a systematic monitoring of a publicly accessible area on a large scale".

The EU Supervisory Authorities are required by Article 35(4) to publish a list of the kind of processing operations that are likely to be high risk and require a DPIA. This list includes a further ten types of processing that automatically require a DPIA:

1. New technologies: processing involving the use of new technologies, or the novel application of existing technologies (including AI).
2. Denial of service: Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data.
3. Large-scale profiling: any profiling of individuals on a large scale.
4. Biometrics: any processing of biometric data.
5. Genetic data: any processing of genetic data other than that processed by an individual GP or health professional, for the provision of health care direct to the data subject.
6. Data matching: combining, comparing or matching personal data obtained from multiple sources.
7. Invisible processing: processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort.

8. Tracking: processing which involves tracking an individual's geolocation or behavior, including but not limited to the online environment.
9. Targeting of children or other vulnerable individuals: The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.
10. Risk of physical harm: Where the processing is of such a nature that a personal data breach could jeopardize the physical health or safety of individuals.

Be aware that the data protection authorities in each EU member states will publish a separate list of types of processing that require a DPIA in their jurisdiction.

The Article 29 working party of EU data protection authorities has published guidelines with nine criteria which may act as indicators of likely high-risk processing:

- Evaluation or scoring.
- Automated decision-making with legal or similar significant effect.
- Systematic monitoring.
- Sensitive data or data of a highly personal nature.
- Data processed on a large scale.
- Matching or combining datasets.
- Data concerning vulnerable data subjects.
- Innovative use or applying new technological or organizational solutions.
- Preventing data subjects from exercising a right or using a service or contract.

In most cases, a combination of two of these factors indicates the need for a DPIA. But it is not a strict rule. If the decision is not to carry out a DPIA because of the confidence that the processing is nevertheless unlikely to result in a high risk, the reasons must be documented.

2.7 New Technologies under GDPR

The GDPR does not define exactly 'new technologies. Recital 91 indicates that this concerns new developments to the state of technological knowledge in the world at large, rather than technology that is new to you. Using technology to process personal data in novel or unexpected ways is likely to be inherently riskier than using technologies that are tried and tested, as the practical implications will not yet be fully understood. This could include the application of artificial intelligence or machine learning within processing operations.

The Article 29 working party guidelines also suggest that the concept of new technologies includes the innovative application of existing technologies to process data in new ways or for new purposes.

If you are planning to use technology you have not used before, even if it is not brand new, it is recommended still to do a DPIA. The technology itself may have been tested by others, but we need to

ensure that we understand the risks and implement it in the most privacy-friendly way – and it may still be considered a 'new technology' if we are actually using the existing technology in a new or innovative way. It may be possible to rely to some extent on any earlier DPIAs carried out on existing technologies by the developer or by another controller who has already put it to use, but it is important to add on an assessment of our own specific implementation plans including the specific nature, scope, purposes and context of processing.

2.8 Definition of Systematic and Extensive under GDPR

GDPR does not directly define 'systematic' or 'systematic and extensive'.

There is some guidance on the meaning of 'systematic' in European guidelines on the DPO provisions. The DPO guidelines say that 'systematic' means that the processing:

- Occurs according to a system
- Is pre-arranged, organized or methodical
- Takes place as part of a general plan for data collection or
- Is carried out as part of a strategy.

The term 'extensive' implies that the processing also covers a large area, involves a wide range of data, or affects a large number of individuals.

2.9 Definition of Significant Affect under GDPR

GDPR does not define the concept of a legal or similarly significant effect. Article 29 working party guidelines on this phrase in the context of profiling provisions give some further guidance.

In short, it is something that has a noticeable impact on an individual and can affect their circumstances, behavior or choices in a significant way.

A legal effect is something that affects a person's legal status or legal rights. A similarly significant effect might include something that affects a person's financial status, health, reputation, access to services or other economic or social opportunities.

Decisions that have little impact generally could still have a significant effect on more vulnerable people, such as children.

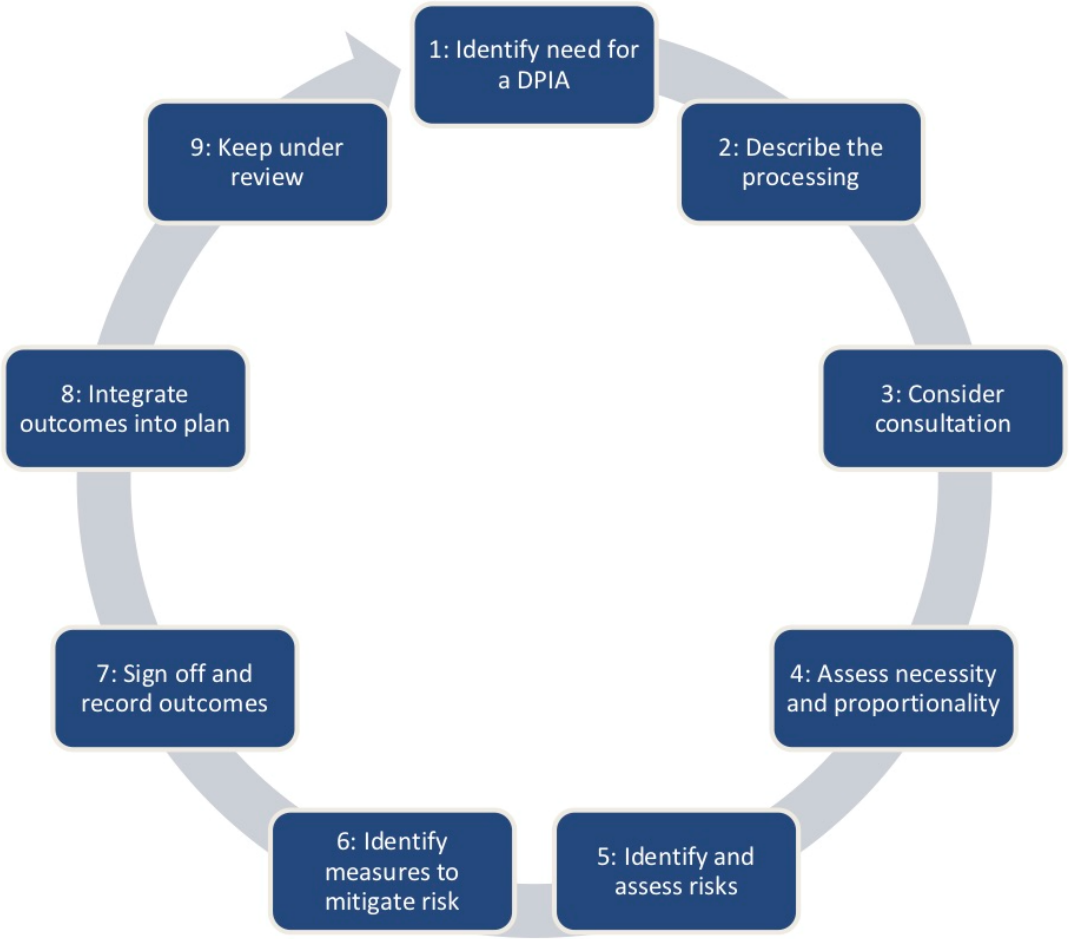
2.10 Definition of Large Scale under GDPR

GDPR does not contain a precise definition of large-scale processing, but to decide whether processing is on a large-scale following should considered:

- The number of individuals concerned
- The volume of data
- The variety of data
- The duration of the processing and
- The geographical extent of the processing. Examples of large-scale processing include:
- A hospital (but not an individual doctor) processing patient data
- Tracking individuals using a city's public transport system
- A fast-food chain tracking real-time location of its customers
- An insurance company or bank processing customer data
- A search engine processing data for behavioral advertising or
- A telephone or internet service provider processing user data.

3 DPIA PROCESS

3.1 Key Elements of the DPIA Process



A DPIA should begin early in the life of a project, before starting processing, and run alongside the planning and development process. It should include these steps:

- Step 1: identify the need for a DPIA
- Step 2: describe the processing
- Step 3: consider consultation
- Step 4: assess necessity and proportionality
- Step 5: identify and assess risks
- Step 6: identify measures to mitigate the risks
- Step 7: sign off and record outcomes
- Step 8: integrate outcomes into project plan
- Step 9: keep your DPIA under review

Individuals and other stakeholders should be consulted as needed throughout this process.

The DPIA process is designed to be flexible and scalable. The process can be designed in a way that fits with an existing approach managing risks and projects, as long as it contains these key elements.

Time and resources needed for a DPIA can also be scaled that it fits to the nature of the project. It does not need to be a time-consuming process in every case.

The three following templates should be used for DPIA:

19e-BM/SG/HDCV/FSOFT	Template_Risk Management DPIA_v3.3
32e-BM/SG/HDCV/FSOFT	Template_DPIA Compact_v1.3

3.2 DPIA, Responsibilities

Responsibility for carrying out DPIAs are FSU/OB heads or GDPO. If FSU/OB head has carried out the DPIA, the GDPO must sign off.

Involved person in a DPIA?

- GDPO
- Risk management team
- Information security
- any processors/sub processor
- LRC, other experts, where relevant.

GDPO should provide advice on:

- whether it is needed to do a DPIA
- DPIA execution, DPIA templates
- whether to outsource the DPIA or do it in-house
- what measures and safeguards have to be taken to mitigate risk
- ensure that the DPIA done correctly
- the outcome of the DPIA and whether the processing can go ahead
- sign off

The advice of the GDPO on the DPIA must be recorded.

GDPOs monitors the ongoing performance of the DPIA, including implementation of planned actions to address the risks.

GDPO must take the overall responsibility for the DPIA.

3.3 Seven Steps of the DPIA Process

3.3.1 Step 1: Decision whether to do DPIA or not

Ask GDPO for advice. If there is any major project which involves the use of personal data, it is best practice to carry out a DPIA.

Check whether the processing is on the list of types of processing which automatically require a DPIA. Screening for other factors which might indicate that it is a type of processing which is likely to result in high risk.

Use the two DPIA checklists.

If the screening exercise is negative and decision is not to do a DPIA, decision and the reasons for it must be documented, including GDPO's advice and approval. This does not have to be an onerous paperwork exercise. For example, simply keep an annotated copy of the checklist

3.3.2 Step 2: Description of the Processing

Description how and why we plan to use the personal data. The description must include "the nature, scope, context and purposes of the processing".

The nature of the processing is what we plan to do with the personal data. This should include, for example:

- How data are collected
- How data are stored
- How data are used
- Who assesses the data?
- Which whom the data are shared with
- Use of any processors/sub processor
- Retention periods
- Security measures
- Use any of new technologies (AI, machine learning, block chain ….)
- Use of any novel types of processing
- Screening criteria flagged as likely high risk

The scope of the processing is what the processing covers. This should include, for example:

- Nature of the personal data
- Volume and variety of the personal data
- Sensitivity of the personal data
- Extent and frequency of the processing

- Duration of the processing
- The number of data subjects involved
- Geographical area covered

The context of the processing is a wider picture, including internal and external factors which might affect expectations or impact. This includes, for example:

- Source of the data
- Nature of the relationship with the individuals
- Extent to which individuals have control over their data
- Extent to which individuals are likely to expect the processing
- Included children or other vulnerable people
- Any previous experience of this type of processing
- Any relevant advances in technology or security
- Any current issues of public concern; and
- In due course, compliance with any GDPR codes of conduct (once any have been approved under Article 40) or GDPR certification schemes.
- Whether we have considered and complied with relevant codes of practice.

The purpose of the processing is the reason why personal data are processed. This includes:

- Legitimate interests, where relevant
- Intended outcome for individuals
- Expected benefits for us or for society as a whole

3.3.3 Step 3: Consulting of Individuals

In most cases it should be possible to consult individuals in some form. If it is decided that it is not appropriate to consult individuals then this decision has to be recorded as part of the DPIA, with a clear explanation. For example, if we are able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.

If the DPIA covers the processing of personal data of existing contacts (for example, existing customers or employees), we have to design a consultation process to seek the views of those particular individuals, or their representatives.

If your DPIA decision is at odds with the views of individuals, we need to document your reasons for disregarding their views.

If a data processor is used, we need to ask them for information and assistance. Contracts with processors should require them to assist.

It is mandatory to consult all relevant internal stakeholders, in particular anyone with responsibility for information security.

Recommend is seeking for legal advice and as well from the risk management team.

In some circumstances we might also need to consult the EU Supervisory Authority after completion of DPIA. That is part of the responsibility of the GDPO.

3.3.4 Step 4: Necessity and Proportionality

To consider:

- Do plans/processing help to achieve the purpose?
- Is there any other reasonable way to achieve the same result?

The Article 29 guidelines say it should be also included how to ensure data protection compliance, which are a good measure of necessity and proportionality. In particular, it should be included relevant details of:

- Lawful basis for the processing
- How to prevent function creep
- How to ensure data quality
- How to ensure data minimization
- How to provide privacy information to individuals
- How to implement and support individuals' rights
- Measures to ensure the processors/sub processor comply
- Safeguards for international transfers.

3.3.5 Step 5: Identification and Assessment of Risks

Consider the potential impact on individuals and any harm or damage that might be caused by the processing – whether physical, emotional, or material. In particular look at whether the processing could possibly contribute to:

- Inability to exercise rights (including but not limited to privacy rights);
- Inability to access services or opportunities
- Loss of control over the use of personal data
- Discrimination
- Identity theft or fraud
- Financial loss
- Reputational damage
- Physical harm
- Loss of confidentiality
- Reidentification of pseudonymized or masked data
- Any other significant economic or social disadvantage

Include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data).

To assess whether the risk is a high risk, both the likelihood and severity of the possible harm must be considered. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than minor, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk.

It must be an 'objective assessment' of the risks.

Structured matrix to check likelihood and severity of risks:

		Catastrophic - 5	Major - 4	Moderate - 3	Minor - 2	Insignificant - 1
		IMPACT				
Almost Certain - 5	LIKELIHOOD	(25) Extreme	(20) Extreme	(15) High	(10) High	(05) Moderate
Most probably - 4		(20) Extreme	(16) Extreme	(12) High	(08) Moderate	(04) Low
Likely - 3		(15) High	(12) High	(09) Moderate	(06) Moderate	(03) Low
Possible - 2		(10) High	(08) Moderate	(06) Moderate	(04) Low	(02) Low
Rare - 1		(05) Moderate	(04) Low	(03) Low	(02) Low	(01) Low

Consider also own corporate risks, such as the impact of regulatory action, reputational damage or loss of public trust.

3.3.6 Step 6: Risk Mitigation Measures

Against each risk identified, record the source of that risk. Consider options for reducing that risk. For example:

- Decision not to collect certain types of data
- Reduction the scope of the processing
- Reducing retention periods
- Additional technological security measures
- Staff training to ensure risks are anticipated and managed
- Anonymizing, pseudonymizing or masking data where possible
- Development of internal guidance or processes to avoid risks
- Addition of a human element to review automated decisions
- Use of different or alternate technology
- Clear data sharing agreements

- Changes to privacy notices
- Offering individuals, the chance to opt out where appropriate
- Implementation of new systems to help individuals to exercise their rights.

DPO must be ask always for advice and approval. Record whether the measure would reduce or eliminate the risk. Take into account the costs and benefits of each measure when deciding whether or not they are appropriate.

3.3.7 Step 7: Conclusion of DPIA

Record:

- what additional measures are planned to take
- whether each risk has been eliminated, reduced, or accepted;
- the overall level of 'residual risk' after taking additional measures; and
- whether you need to consult the EU Supervisory Authorities (e.g., ICO).

You do not always have to eliminate every risk. You may decide that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of mitigation. However, if there is still a high risk, you need to consult the EU Supervisory Authorities e.g., ICO) before you can go ahead with the processing.

As part of the sign-off process, GDPO advises and approves whether the processing is compliant and can go ahead.

3.3.8 Next Steps

Incorporation of the outcomes of the DPIA back into the project/ processing plans. Identify any action points and who is responsible for implementing them. The project management process should be used to ensure these are followed through.

Monitoring of the ongoing performance of the DPIA should be implemented. Maybe there is the need to cycle through the process again before the plans are finalized.

If it is decided to accept a high risk, either because it is not possible to mitigate or because the costs of mitigation are too high, we need to consult the EU Supervisory Authorities (e.g., ICO) before we can go ahead with the processing.

It is good practice to publish DPIA to aid transparency and accountability. This could help foster trust in our processing activities and improve individuals' ability to exercise their rights. If there are concerned that publication might reveal commercially sensitive information, undermine security, or cause other risks, it should be considered whether to redact (black out) or remove sensitive details, or publish a summary.

DPIA needs to keep under review, and maybe needs to repeat it if there is a substantial change to the nature, scope, context or purposes of the processing.

4 SIMPLE CHECKLISTS (example)

4.1 DPIA Screening Checklist

- Carry out a DPIA if we plan to:
    - Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
    - Process special category data or criminal offence data on a large scale.
    - Systematically monitor a publicly accessible place on a large scale.
    - Use new technologies.
    - Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
    - Carry out profiling on a large scale.
    - Process biometric or genetic data.
    - Combine, compare, or match data from multiple sources.
    - Process personal data without providing a privacy notice directly to the individual.
    - Process personal data in a way which involves tracking individuals' online or offline location or behavior.
    - Process children's personal data for profiling or automated decision-making or for marketing purposes or offer online services directly to them.
    - Process personal data which could result in a risk of physical harm in the event of a security breach.
- Consider whether to do a DPIA if it is planned to carry out any other:
    - Evaluation or scoring.
    - Automated decision-making with significant effects.
    - Systematic monitoring.
    - Processing of sensitive data or data of a highly personal nature.
    - Processing on a large scale.
    - Processing of data concerning vulnerable data subjects.
    - Innovative technological or organizational solutions.
    - Processing involving preventing data subjects from exercising a right or using a service or contract.

- If it is decided not to carry out a DPIA, document the reasons.
- Consider carrying out a DPIA in any major project involving the use of personal data.
- Carry out a new DPIA if there is a change to the nature, scope, context, or purposes of our processing.

4.2 DPIA Process Checklist

- Description of the nature, scope, context, and purposes of the processing.
- Consultation of the data processors to help to understand and to document their processing activities and identify any associated risks.
- Consider how best to consult individuals (or their representatives) and other relevant stakeholders.
- Ask the data protection officer for advice, Follow GDPO's advice.
- Check that the processing is necessary for and proportionate to the purposes. Description how we to ensure data protection compliance.
- Objective assessment of the likelihood and severity of any risks to individuals' rights and interests.
- Identification of measures which can be put in place to eliminate or reduce high risks.
- Record the outcome of the DPIA, including any difference of opinion with our GDPO or individuals consulted.
- Implementation of identified measures, and integration of them into the project plan.
- Consultation of the EU Supervisory Authorities (ICO) before processing if the high risks cannot be mitigated.

5 APPENDIXES

5.1 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

5.2 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

5.3 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.