



GDPR VS THE WORLD

PART 1 GDPR VS ASIA



Thailand 

Malaysia

China

Hong Kong

Japan

Singapore

India

South Korea

Indonesia

UAE

How much has the GDPR driven data protection worldwide ?

An in-depth comparison of different legislations
around the world based on 35 criteria

Authors



Stéphanie Exposito-Rosso
IT Legal Expert and Main Author



Sumedha Ganjoo
Legal Research Lead



Katia Bouslimani
Chief Legal Research Officer



Adam Ali-Bey
IT Legal Expert



Antoine Piquet
IT Legal Expert



Eloïse Quinzin
IT Legal Expert

We would like to thank Bianca Kunrath, Era Selmani and Ylli Kodza for their feedback. Copy editing, report design, and support for content strategy was provided by platformable.com

The information provided in this publication is general and may not apply in a specific situation. The publishers and authors accept no responsibility for any acts, errors or omissions contained herein. The information provided was verified between October 2021 and August 2022. Note that the regulation is meant to evolve.

The following report is the result of Code is Law (Alias.dev)'s research, including interviews with local professionals, who asked to be cited anonymously. We also interviewed Mr Montri Stapornkul, Data Protection Officer at Dtac, who kindly specified important points of the PDPA.

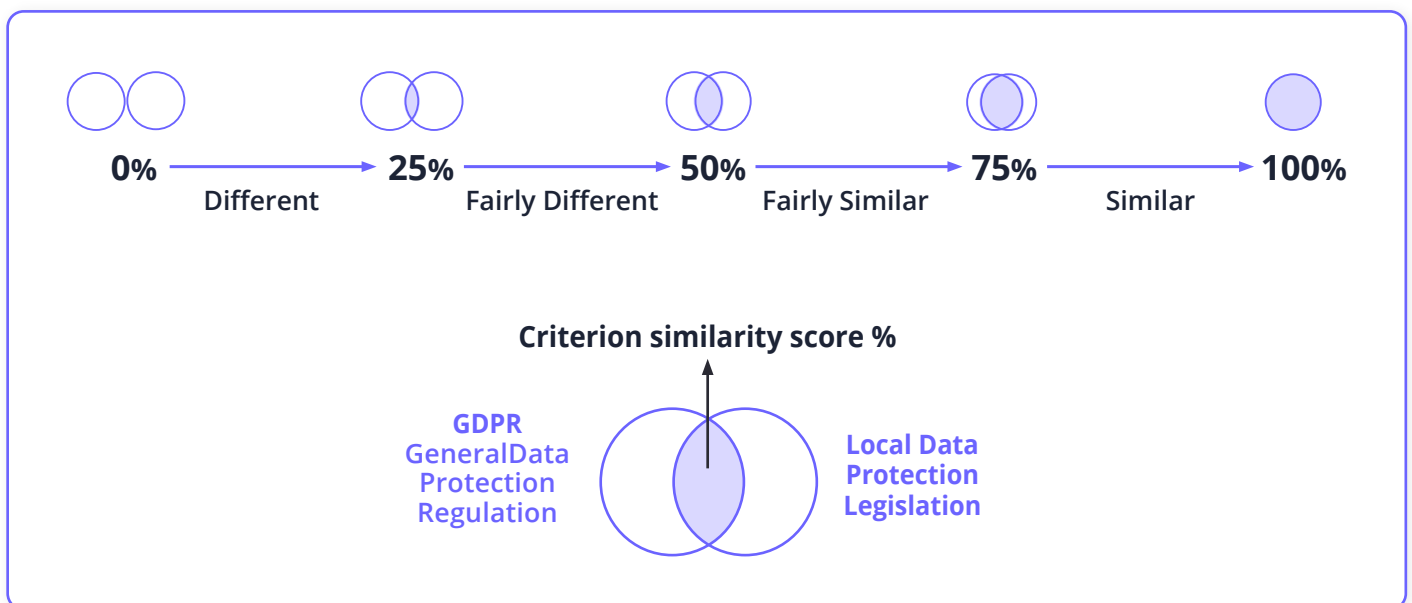
Published September 2022

Welcome to the “GDPR VS” Series

The General Data Protection Regulation (GDPR) was adopted in 2016 by the European Parliament and the European Council, and entered into force on 25 May 2018. Innovative by its extensive scope, provisions and enforcement potential, the GDPR made a lot of noise and required companies to provide efforts of compliance.

25 May 2022 is the fourth anniversary of the GDPR, and a pertinent time to ask: Has the GDPR created “a recipe for the world?” [Code is Law \(Alias.dev\)](#) aims to assess the level of influence of the GDPR in different regions of the world that have adopted or have not adopted new data protection regulations since 2016. The objective is to help companies conduct their gap analysis between different data protection legislations in their data protection compliance efforts.

[Alias.dev](#) chose 35 criteria to compare the GDPR with other data protection legislation, and analysed these criteria through more than 200 sub-criteria. Each criterion is given a similarity score. The score indicates how much effort GDPR-compliant companies will have to engage to comply with data protection legislation outside the EU and understand the data protection culture of the jurisdiction. The similarity score is as follows:



35 Criteria
divided into
7 Categories

- Scope
- Lawfulness
- Data Subjects’ Rights
- Accountability Requirements
- Data Localisation and Transfer
- Enforcement
- Exemptions

Criteria 1–5	●●●●●
Criteria 6–10	●●●●●
Criteria 11–18	●●●●●●●●
Criteria 19–27	●●●●●●●●●●
Criteria 28–29	●●
Criteria 30–31	●●
Criteria 32–35	●●●●

Contents

05 List of Acronyms

06 Introduction

07 Scope

Criterion 1. The Territorial Scope /7

Criterion 2. The Subject Matter Scope /8

Criterion 3. Definition of Personal Data /9

Criterion 4. Definition of Sensitive Personal Data /10

Criterion 5. Relevant Parties /11

13 Lawfulness

Criterion 6. Legal Bases /13

Criterion 7. Consent /14

Criterion 8. Legitimate Interest /15

Criterion 9. Conditions for Processing of Sensitive Data /16

Criterion 10. Children /17

18 Data Subjects' Rights

Criterion 11. Transparency Requirements /18

Criterion 12. Right of Access /19

Criterion 13. Right to Data Portability /20

Criterion 14. Right to Rectification /21

Criterion 15. Right to be Forgotten / Right to erasure /22

Criterion 16. Right to Object /23

Criterion 17. Rights Related to Profiling /24

Criterion 18. Right to Restrict the Use of the Personal Data /24

25 Accountability Requirements

Criterion 19. Appointment of a Representative /25

Criterion 20. Appointment of a DPO /26

Criterion 21. Record of processing /28

Criterion 22. Data Protection Impact Assessment (DPIA) /29

Criterion 23. Privacy by Design / Right to Erasure /30

Criterion 24. Audit Requirements /30

Criterion 25. Appointment of Processors /31

Criterion 26. Information Security /32

Criterion 27. Breach Notification /33

34 Data Localisation and Transfer

Criterion 28. Data Localisation Requirements /34

Criterion 29. International Data Transfer /34

36 Enforcement

Criterion 30. Data Protection Authority /36

Criterion 31. Penalties /38

39 Exemptions

Criterion 32. Anonymised Data /39

Criterion 33. Social Media Intermediaries and Identity Managements /39

Criterion 34. Exemptions for Research /40

Criterion 35. Application to Public Authorities /41

42 Conclusion

43 Compliance-as-Code: Our Solution

List of Acronyms

D

DPO: Data Protection Officer

DPIA: Data Protection Impact Assessment

G

GDPR: General Data Protection Regulation

J

JSCCIB: Joint Standing Committee on
Commerce, Industry and Banking

P

PDPA: Personal Data Protection Act

PDPC: Personal Data Protection Committee

R

ROPA: Record of Data Processing Activities

Introduction

On 27 May 2019, Thailand published its first personal data protection law, the Personal Data Protection Act (PDPA), in the Royal Thai Government Gazette. It is Thailand's first-ever data privacy legislation and is understood to have been influenced by the GDPR.

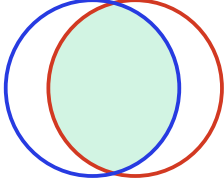
The PDPA was scheduled to go into effect on 27 May 2020. However, due to the COVID-19 pandemic, the entry into force was postponed to 27 May 2021. On 5 May 2021, it was then pushed to 1 June 2022. The Ministry of Economy and Digital Society (MDES) stated that due to the pandemic, companies and operators were already suffering a significant cost, which would be increased with the entry into force of the PDPA. The professionals interviewed stressed that they are waiting for guidelines in order to facilitate the implementation of the Act. Finally on 1 June 2022, Thailand's Personal Data Protection Act ("PDPA") entered into force. On 20 June 2022, the Personal Data Protection Commission ("PDPC") announced the first set of supplementary laws under the PDPA in the Royal Gazette.

The four supplementary laws (collectively, the "PDPA Notifications") include exemptions for certain small and medium-sized enterprises, responsibilities of Data Processors on storage and safeguarding activities, and administration of penalties for violations of the PDPA.

The protection of personal data is closely linked to the notion of privacy. The Thai constitution enshrines the right to privacy, and enshrines the right to respect for dignity, reputation and family. The Thai Constitution is not the only text that governs the issue of privacy and personal data. Indeed, there are:

- The Notification of the Ministry of Digital Economy and Society Re: Personal Data Protection Standards B.E. 2563
- The Cybersecurity Act, B.E. 2562
- The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications
- The Credit Information Business Act B.E. 2545
- The National Health Act B.E. 2550
- The Payment System Act B.E. 2560
- The Official Information Act B.E. 2540
- The Thai Civil and Commercial Code
- The International Covenant on Civil and Political Rights (1966)
- The ASEAN Human Rights Declaration (2012)

Under the PDPA, the supervisory authority responsible for monitoring compliance with the Act is the Personal Data Protection Committee (PDPC), under the Minister of Digital Economy and Society. The establishment of the PDPC was completed in January 2022, in order to be ready for the full enforcement of the PDPA in June 2022.

Scope	 <p>75%</p>	Similar
Criterion 1. The Territorial Scope		

GDPR

Article 3

The GDPR is applicable when there is the presence of an “establishment” in the EU, which means that the Data Controller or the Data Processor exercises an effective and real activity (even a minimal one) through stable arrangements.

Extraterritorial scope: applies when a Data Controller or a Data Processor that is located outside the EU processes activities that are related to the offering of goods or services (regardless of the existence of a payment) to Data Subjects in the EU or to the monitoring of their behaviour as far as their behaviour takes place within the EU.

Section 5

PDPA

The PDPA governs the acquisition, use, and disclosure of personal data by Thai-based organisations, regardless of whether the data is collected, used, or disclosed in Thailand.

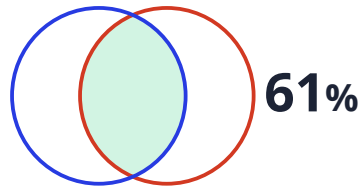
Extraterritorial scope: applies to Data Controllers and Data Processors based outside of Thailand who collect, use, or disclose personal data of Thai Data Subjects in connection with the offering of goods or services to Thai Data Subjects, regardless of whether payment is required, or where the Data Subject’s behaviour is being monitored in Thailand.

Regarding territorial scope, the PDPA and the GDPR equally treat establishments in terms of presence in their territories.

Regarding extraterritorial application, the GDPR applies to Data Controllers and Data Processors who do not have a physical presence in the EU, but conduct processing operations there. Similarly, if their operations include supplying goods or services to, or monitoring the behaviour of, Data Subjects in Thailand, the PDPA applies to Data Controllers and Data Processors located outside of Thailand.

Scope

**Criterion 2.
The Subject Matter Scope**



Fairly Similar

 **GDPR** **Article 1**

The GDPR's aims are clearly defined: to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data and to protect and encourage the free movement of personal data within the EU.

If the data is part of a file system, the GDPR applies to the processing of personal data by automated or non-automated methods.

The GDPR does not apply to anonymised data.

The GDPR exempts:

- Personal data processed by people for solely personal or domestic reasons that has "no relation to a professional or commercial activity".
- Data processed in the context of law enforcement or national security.

The GDPR establishes standards for some types of processing, such as processing for journalistic purposes and processing for academic, artistic, or literary expression.

Preamble, Section 4  **PDPA**

The PDPA's aims are stated in the Act: "to efficiently protect personal data and put in place effective remedial measures for Data Subjects whose rights to the protection of personal data are violated".

The PDPA does not specify the material scope of the Act. Therefore, the PDPA seems to apply to any collection, use, or disclosure of personal data, regardless of whether the data is part of a file system and/or whether it is processed by automated or non-automated methods.

The PDPA does not seem to apply to anonymised data.

The PDPA exempts:

- Personal data processed by an individual for personal benefit or household activity of such an individual.
- Personal data processed by public authorities that have the duties to maintain State security, including financial security of the State or public safety, including the duties with respect to the prevention and suppression of money laundering, forensic science or cybersecurity.
- Personal data processed for the activities of mass media, fine arts, or literature, which are only in accordance with professional ethics or for public interest.
- Trial and adjudication of courts and work operations of officers in legal proceedings, legal execution, and deposit of property, including work operations in accordance with the criminal justice procedure.
- Operations of data undertaken by a credit bureau company and its members, according to the law governing the operations of a credit bureau business.

Both laws allow personal data to be processed for legal reasons, for personal use, and for certain creative and media purposes. Anonymised data is exempted from the provision of both texts.

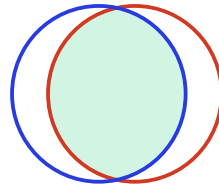
In terms of material scope, the PDPA only refers to the collection, use, or disclosure of personal data. On the other hand, the GDPR specifies that it applies to the processing of personal data by automated and non-automated methods, as long as the data is part of a file system.

The scopes for both the GDPR and the PDPA exempt the processing of personal data for personal or domestic purposes, and the processing of personal data in the context of law enforcement or national security.

Contrary to the GDPR, legislative entities and credit bureaus are also exempted from the scope of the PDPA.

Scope

**Criterion 3.
Definition of Personal Data**



80%

Similar

 **GDPR** Article 4, (1), (13), (14), (15), Article 9

Personal data is defined by the GDPR as:


- Any information relating to an identified or identifiable natural person (“Data Subject”).

An identifiable natural person, according to the GDPR, 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 one or more factors specific to that natural person’s physical, physiological, genetic, mental, economic, cultural, or social identity.

Online identifiers, such as IP addresses, cookie identifiers, and radio frequency identifying tags, are considered personal data under the GDPR.

The GDPR does not apply to deceased people.

The GDPR does not apply to data that has been “anonymised” that can no longer be used to identify the Data Subject.

Section 6  **PDPA**

The PDPA defines “personal data” as:

- Any information about a person that may be used to identify that person, whether directly or indirectly, with the exception of information about people who are deceased.

A “person”, according to the PDPA, is defined as a “natural person.”

IP addresses, cookie IDs, and radio frequency identification tags are not directly addressed by the PDPA.

The PDPA does not explicitly exclude anonymised data from its scope but it defines anonymous data as data “which cannot identify the Data Subject”. It seems to be an implicit exclusion of anonymised data.

Both the GDPR and PDPA define personal data as information that relates directly or indirectly to an individual. They both provide specific criteria for certain categories of data, and apply to the collection, use, and disclosure of personal data.

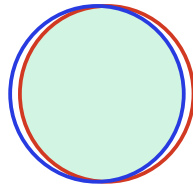
The GDPR provides a more comprehensive definition, including IP addresses, cookie identifiers, and radio frequency identification tags as personal data.

As for similarities, both regulations do not apply to the data of persons who are deceased.

Contrary to the GDPR, the PDPA does not explicitly exclude anonymised data from its scope, but its exclusion seems to be implied. According to interviewed professionals, a regulation specific to anonymisation is being elaborated.

Scope

Criterion 4. Definition of Sensitive Personal Data



95%

Similar

 **GDPR**

Article 9

The GDPR's definition of sensitive personal data covers:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- The processing of genetic data and biometric data for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation

Section 26

PDPA 

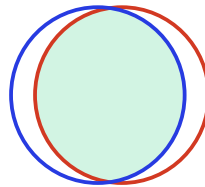
The PDPA's definition of sensitive personal data covers:

- Racial or ethnic origin
- Political opinions
- Cult, religious or philosophical beliefs
- Sexual behaviour
- Criminal records
- Health data and disability
- Trade union information
- Genetic data, biometric data or any data which may affect the Data Subject in the same manner

The GDPR and the PDPA provide very similar definitions of sensitive personal data. The PDPA includes criminal records in sensitive data, for which the GDPR has specific, applicable provisions.

Scope

**Criterion 5.
Relevant Parties**



88%

Similar

 **GDPR** **Article 4 (7), 28, 30, 82**

- A Data Controller is a natural or legal person, public authority agency, or other organisation that, alone or collectively with others, decides the goals and methods of processing personal data.

- A Data Processor is a natural or legal person, government agency, or other entity that processes personal data on behalf of the Data Controller.


Data Controllers must adhere to the purpose restriction and accuracy principles, and repair any inaccurate or incomplete personal data held by a Data Subject. They are required to put in place technological and organisational security measures, and alert supervisory authorities in the event of a data breach.

Data Controllers and Data Processors are required to retain records of processing operations, although small businesses are exempt from this need. Data Controllers and Data Processors can also designate a DPO.

Where processing is carried out on behalf of a Data Controller, the Data Controller must only use Data Processors who can provide sufficient guarantees to implement the appropriate technical and organisational measures to ensure that processing complies with the GDPR's requirements and protects the Data Subject's rights. Furthermore, without the Data Controller's previous explicit or general written authorisation, the Data Processor may not engage another Data Processor.

No examination system is named. However, the GDPR states that "time limits for erasure or periodic review should be established by the Data Controller".

In specific cases, the GDPR requires a Data Controller or Data Processor to complete a DPIA.

Section 6  **PDPA**

- A Data Controller is a natural person or a legal entity with the authority and responsibility to make decisions about the collection, use, and disclosure of personal data.

- A Data Processor is a person or a juristic person who operates in relation to the collection, use, or disclosure of personal data pursuant to orders given by or on behalf of a Data Controller.

Data Controllers are required to keep "accurate, up-to-date, full, and not misleading" personal data. In addition, the PDPA states that "the collecting of personal data should be restricted to the amount required in relation to the Data Controller's authorised purpose".

Data Controllers or Data Processors must implement suitable security measures that fulfil the PDPC's minimal standards, and these measures must be reviewed as needed. The PDPA also requires Data Controllers inform the PDPC in the event of a data breach.

When "personal data is to be supplied to other people or legal persons, apart from the Data Controller," the PDPA states, "the Data Controller should take steps to prevent such person from using or disclosing such personal data illegally or without authorisation".

Data Controllers must set up an examination system for deletion or destruction of personal data as needed to comply with retention periods, when a Data Subject withdraws permission, and so on.

DPIAs are not specifically mentioned in the PDPA.

Section 37(1), on the other hand, states that Data Controllers have a responsibility to establish sufficient security measures and to assess such measures as needed or when technology changes in order to successfully maintain suitable security and safety requirements.

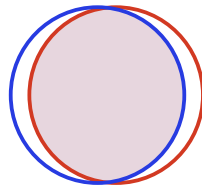
The scope and duties of Data Controllers and Data Processors are identical in the GDPR and the PDPA, with equivalent definitions and requirements for Data Subject rights, data breach notifications, record keeping, security measures, and the appointment of a Data Protection Officer (DPO).

Data Controllers must take sufficient security measures and inform supervisory authorities of data breaches under both the GDPR and the PDPA.

While the GDPR requires Data Controllers to conduct Data Protection Impact Assessments (DPIA) in certain circumstances, the PDPA states that Data Controllers must implement appropriate security measures and review them as needed or as technology evolves in order to effectively maintain appropriate security and safety standards.

Lawfulness

Criterion 6. Legal Bases



90%

Similar



GDPR

Articles 6-10 Recitals 39-48

Processing is lawful only if and to the extent that at least one of the following applies:

- The Data Subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the Data Subject is a child.

Section 24

PDPA 

In the PDPA, consent is the legal basis by default for the processing of personal data.

The Data Controller shall not collect personal data without the consent of the Data Subject unless:

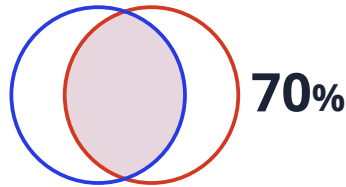
- It is necessary for the performance of a contract to which the Data Subject is a party, or in order to take steps at the request of the Data Subject prior to entering into a contract.
- It is necessary for compliance with a law to which the Data Controller is subjected.
- It is for preventing or suppressing a danger to a person's life, body or health.
- It is necessary for the performance of a task carried out in the public interest by the Data Controller, or it is necessary for the exercising of official authority vested in the Data Controller.
- It is necessary for legitimate interests of the Data Controller or any other persons or legal persons other than the Data Controller, except where such interests are overridden by the Data Subject's fundamental rights concerning their personal data.
- It is for the achievement of the purpose relating to the preparation of historical documents or archives for public interest, or for the purpose relating to research or statistics, in which suitable measures to safeguard the Data Subject's rights and freedoms are put in place and in accordance with a Notification as prescribed by the PDPC.

A notable difference here is that for the PDPA, consent is the cornerstone. In fact, consent applies first and then other legal bases. Another difference is that the GDPR has six legal bases, and the PDPA has seven.

The legal bases are relatively similar, even if the semantics sometimes differ. The PDPA has an additional legal basis which is the one for historical purposes, public interest purposes, research purposes, and statistics purposes. It is interesting to note that these purposes are subject to derogative rules in the GDPR, but do not constitute a legal basis.

Lawfulness

Criterion 7. Consent



Fairly Similar



GDPR

Articles 4(11), 7, Recitals 32,
42, 43

The GDPR establishes a set of criteria for gaining valid consent:

- Consent must be freely given, specific and informed.
- It must be granted by an unambiguous, affirmative action where the Data Subject signifies agreement to the processing of personal data relating to them.
- Generally, provision of a service cannot be made conditional on obtaining consent for processing that is not necessary for the service.
- A request for consent must be distinct from any other terms and conditions.
- The consent can be easily withdrawn at any moment “without prejudice”.

Sections 19, 24, 26, 27

PDPA 

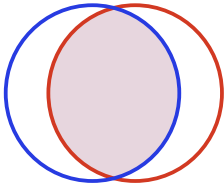
In the PDPA, the criteria for consent are:


- The Data Controller shall make every effort to ensure that the consent of the Data Subject is freely given.
- The Data Controller is bound to inform the Data Subject about the purpose of the processing.
- The request for consent is required to be easily accessible, intelligible, using clear and plain language. It should not be deceptive or misleading to the Data Subject.
- The request for consent shall be explicitly made in a written statement or via electronic means, unless it cannot be done due to its nature.
- Data Subjects can withdraw their consent at any time, in an easy way (as easy as for giving consent).

Consent is the primary legal foundation for the PDPA. Concerning the criteria, both laws make reference to consent requirements.

The GDPR expressly defines consent as a demonstration of free, specific, clear, and informed will. In the PDPA, consent must be freely given, the Data Subject must be informed of the purpose of the processing, and the request for consent must not be deceptive or misleading. However, there is no provision about the specific nature of the consent request.

Both the GDPR and the PDPA establish the right for Data Subjects to withdraw their consent at any time.

Lawfulness	 <p>75%</p>	Similar
Criterion 8. Legitimate Interest		



GDPR

Recital 47, Articles 7, 21

Processing is permitted where it is necessary for the Data Controller (or a third party's) legitimate interests and provided such interests are not overridden by the Data Subject's rights and interests.

It is the Data Controller's responsibility to determine whether the interests it pursues under this basis are legitimate and proportionate, and Data Controllers are expected to document their assessments.

Section 24

PDPA


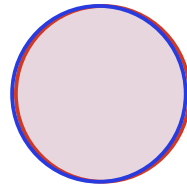
Processing is permitted when it is necessary for the legitimate interests of the Data Controller or any other person, except when such interests are overridden by the Data Subjects' fundamental rights concerning their personal data.

In case of a Data Subject exercising their right to object the processing, the Data Controller is required to demonstrate compelling legitimate ground in order to process the personal data.

Legitimate interest is a valid legal basis in both texts. In both cases, the Data Controller can rely on their legitimate interests when they can demonstrate that they are not overridden by the Data Subject's rights. The GDPR is more demanding as it also requires the Data Controller's legitimate interest not to be overridden by the Data Subject's interests.

Lawfulness

Criterion 9. Conditions for the Processing of Sensitive Data



99%

Similar

GDPR

Articles 9, 10, Recital 47

There are ten legal bases for processing sensitive data, subject to further additions by Member States:

1. Explicit consent.
2. To comply with obligations and exercising rights in the context of employment and social security.
3. Life protection and vital interests.
4. Legitimate activities (by a foundation, association or other non-profit body with a political, philosophical, religious, or trade union aim, which processes data about its members).
5. Establishment, exercise, or defence in legal claims.
6. Data manifestly made public by the individual.
7. Substantial public interest defined by law.
8. Preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment.
9. Substantial public interest in health.
10. Archiving, scientific, or historical research purposes.

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of Data Subjects. Any comprehensive register of criminal convictions shall be kept only under the control of an official authority.

Section 26

PDPA

There are also ten legal bases for processing sensitive data in the PDPA:

1. Explicit consent.
2. Employment protection, social security, national health security, social health welfare of the person, road accident victims protection, social protection.
3. Vital interest.
4. Legitimate activities (by a foundation, association or other not-for-profit body with a political, philosophical, religious, or trade union aim, which processes data about its members).
5. The establishment, defence, exercise or compliance of legal claims.
6. Data clearly made public by the Data Subject.
7. Substantial public interest.
8. Preventive medicine or occupational medicine, assessment of working capacity of the employee, medical diagnosis, the provision of health or social care, medical treatment, the management of health or social care systems and services.
9. Public interest in health.
10. Scientific or historical research purposes.

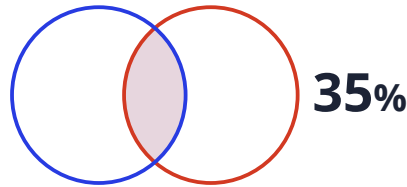
The collection of personal data relating to criminal record must be carried out under the control of an authorised official authority under the law, or be protected by measures implemented by the Data Controller according to the rules prescribed by the PDPC.

Both the GDPR and the PDPA generally prohibit the processing of sensitive data. This prohibition, however, may be abolished if one of the listed requirements is satisfied. The GDPR and the PDPA provide very similar legal bases for the processing of sensitive personal data.

Like the GDPR, the PDPA requires that personal data linked to criminal records are collected under the supervision of an authorised official authority. But unlike the GDPR, the data protection measure is implemented in accordance with guidelines specified by the PDPC.

Lawfulness

Criterion 10. Children



Fairly Different



GDPR

Articles 6, 8, 12, 40, 57,
Recitals 38, 58, 75

The GDPR doesn't define the terms "child" or "children". However, children are considered "vulnerable natural people" under the GDPR, who need special protection when it comes to their personal data.

For delivering information society services to a child under the age of 16, the consent of a parent or guardian is necessary if the processing is based on consent. This age restriction may be lowered to 13 by EU member states.

When children's personal data is used for marketing or gathered for information society services presented directly to children, special protection should be provided.

Where any information is intended exclusively for a child, Data Controllers shall take necessary means to convey information relevant to processing in a brief, transparent, comprehensible, and readily available manner, using clear and simple language that the child may easily comprehend.

In the case of information society services, the GDPR's requirements on the appropriate circumstances for processing children's data apply.

Chapter II, part 1, Section 20

PDPA 

The PDPA doesn't define the terms "child" or "children".

However, there are some special protections when it comes to their personal data.

If a minor is under ten, consent must be obtained from the child's holder of parental responsibility. The holder of parental responsibility's consent is also required when minors (under 20) are older than ten, but they are not competent to give their consent under Thai law.

The PDPA does not clarify if children's personal data should be protected, whether it is used for marketing or gathered for information society services provided directly to them.

The PDPA does not specify what steps Data Controllers must take when speaking or delivering information to a child.

The PDPA does not state whether Data Controllers must take reasonable measures to verify that parental or guardian permission has been granted.

Both the GDPR and the PDPA include specific requirements for safeguarding children's data, but such requirements differ.

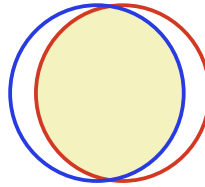
The PDPA requires the Data Controller to obtain parental or guardian approval when children are under the age of ten. Over the age of ten, the Data Controller may solely ask for the minor's consent when the minor is competent to give consent according to Thai law. If the minor is not competent to give consent, the Data Controller requires the minor's consent as well as parental or guardian consent until the age of 20.

In the GDPR, the holder of parental responsibility's consent is required when the child is under 16, with Member States having the option to lower the age limit to 13.

Unlike the PDPA, the GDPR establishes particular criteria for delivering information to children, and stipulates that children's personal data shall be protected, whether it is used for marketing or gathered for information society services provided directly to children.

Data Subjects' Rights

**Criterion 11.
Transparency Requirements**




85%

Similar

 **GDPR** **Article 12, Recital 58**

The GDPR explicitly refers to the principle of transparency, which involves providing information to the Data Subject. The information must be “concise, easily accessible and easy to understand” through the use of “clear and simple language”.

The information to be provided is precisely detailed in the GDPR.

Section 23 **PDPA** 

Section 23 states that the Data Controller must inform the Data Subject about the collection of their data.

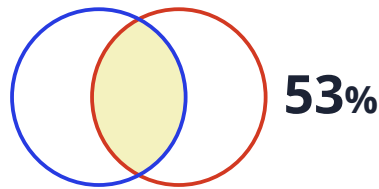
It specifies that this information must be given before or at the time of collection, except “in the event that the Data Subject already knows these details”.

The information to be provided is precisely detailed in the PDPA.

The notion of transparency is recognised by both the GDPR and the PDPA. These two regulations require the Data Controller to provide certain information to Data Subjects about the acquisition and processing of their personal data.

Data Subjects' Rights

Criterion 12. Right of Access



Fairly Similar

GDPR

Articles 12, 15, Recitals 59-64

Data Subjects have the right to access the personal data that is processed by a Data Controller.

According to the GDPR, the Data Controller must provide the following information when responding to an access request:

- The recipients or categories of recipients to whom the personal data has been or will be disclosed, in particular recipients in third countries or international organisations.
- The envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
- The existence of the right to request rectification from the Data Controller.

According to the GDPR, the right of access shall not infringe on others' rights or freedoms, particularly those connected to trade secrets.

Requests from Data Subjects under this right must be responded to without "undue delay" and in any case within one month of receipt.

The right to access is unrestricted. A charge may be required in certain cases, particularly when the demands are unwarranted, unreasonable, or recurrent.

Data Subjects must be able to submit their requests in a number of ways, including verbally and by technological means. In addition, when a request is made using electronic means, the Data Controller shall respond via electronic means as well.

Section 30

PDPA

Data Subjects have the right to access their personal data that is processed by a Data Controller under the PDPA. The right to access personal data and seek a copy of such data shall not infringe on the rights or freedoms of others, according to the PDPA.

The PDPA does not specify what must be provided in an access request response.

A Data Controller may only deny a request for access to personal data, including obtaining a copy and/or source of personal data, if the denial is legal or if a court order requires it.

There are no exceptions to the PDPA when it comes to trade secrets.

A Data Controller shall reply to the request without undue delay, and no later than 30 days after receiving it, with no additional period. However, Notification(s) from the competent authorities pertaining to the exercise of rights as well as a term of extension may be issued in the future.

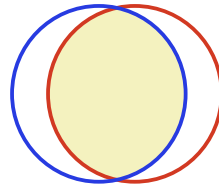
The PDPA does not state if this privilege may be exercised for free. The PDPA does not clarify how Data Subjects might seek access to their personal information. However, the competent authority's Notification(s) pertaining to the exercise of rights, which may include the cost of implementation, may be published in the future.

Both the GDPR and the PDPA provide Data Subjects with the right to access their personal data when it has been collected and processed by a Data Controller. However, the laws have several differences with regard to the implementation of the right to access. For instance, the grounds for denying the right of access to some personal data differ.

Also, the GDPR precisely details the implementation of the right of Data Subjects to access their personal data whereas the PDPA lacks some specifications. These specifications, such as the cost of the data access request, may be published in the future.

Data Subjects' Rights

**Criterion 13.
Right to Data Portability**



80%

Similar

 **GDPR** **Article 20**


Data Subjects have the right to data portability under the GDPR.

When processing is based on consent or contract, and is processed through automated methods, Data Subjects have the right to obtain their personal data in a structured, generally used, and machine-readable format.

Where technically practicable, Data Subjects have the right to send their personal data in the aforementioned form directly to another Data Controller.

The GDPR provides that the right to data portability shall not jeopardise other people's rights or freedoms.

The GDPR does not make it mandatory for a Data Controller to keep a record of the reasons presented for refusing a data portability request.

Section 31 **PDPA** 

Data Subjects have the right to data portability under the PDPA.

When processing is based on consent, contract, or a legitimate reason, Data Subjects have the right to obtain their personal data in a structured, frequently used, and machine-readable format.

Data Subjects have the right to request that a Data Controller:

- Directly send their personal data in the aforementioned form to another Data Controller.

Or

- Disclose the sent data, if technically practicable.

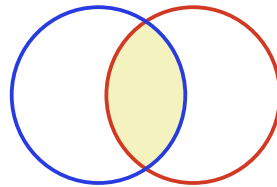
The right to data portability shall not infringe on the rights or freedoms of others.

The Data Controller must keep a record of the reason for an objection to a data portability request so that Data Subjects and the competent authority may verify it.

Both the GDPR and the PDPA recognise the right to data portability. Under these two laws, Data Subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format as well as to transmit such data to other third parties. One difference is that under PDPA, the Data Controller has to keep track of the reason for an objection to a data portability request so that Data Subjects and the competent authority may verify it, whereas it is not mandatory under GDPR.

Data Subjects' Rights

Criterion 14. Right to Rectification



45%

Fairly Different



Article 16

Data Subjects have the right to correct inaccurate personal data and complete incomplete personal data.

Where personal data is updated, it must be communicated to each recipient to which it was disclosed, unless this would involve disproportionate effort.

The Data Controller must restrict processing where the accuracy of the data is disputed for the time needed to verify the request.

Sections 35, 36, 37



The PDPA requires Data Controllers to ensure that the personal data remains accurate, up-to-date, complete and not misleading.

Data Subjects may request Data Controllers to act in compliance with the obligation of accuracy of personal data.

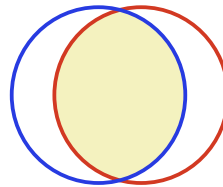
When it does not take action following such a request, the Data Controller is required to keep such request in a record.

In both the GDPR and PDPA, it is the responsibility of the Data Controller to ensure that the data is accurate.

However, the logic of rectification requests differs. The GDPR explicitly mentions that the Data Subject has the right to have their data corrected and completed. On the other hand, under the PDPA, the Data Controller is required to ensure that the personal data remains accurate, up-to-date, complete, and not misleading, and the Data Subject can request the Data Controller to comply with this requirement.

Data Subjects' Rights

Criterion 15.
Right to be Forgotten /
Right to Erasure



75%

Similar

 **GDPR**

Articles 12, 17 Recitals 59, 65-66

The right to be forgotten applies to specific circumstances, such as when a Data Subject's consent is revoked and there is no other legal basis for processing, or when personal data is no longer required for the purposes for which it was obtained.

The right to erasure/to be forgotten is unrestricted. However, there are certain circumstances in which a charge may be demanded, such as when demands are baseless, unreasonable, or frequent.

If the Data Controller has made personal data public and is required to erase the personal data, the Data Controller shall take reasonable steps, including technical measures, to notify Data Controllers processing the personal data that the Data Subject has requested the erasure by such Data Controllers of any links to, or copy or replication of those personal data, taking into account the available technology and the cost of implementation.

The GDPR sets out exceptions to the right to erasure in the case of:

- Conflict with freedom of speech and information.
- Compliance with public interest objectives in the field of public health.
- Creation, exercise, or defence of legal claims.
- Compliance with legal duties for a public interest purpose.

Under this right, Data Subject requests must be responded to "without excessive delay and in any case within one month of receipt of request".

Section 33

PDPA 

When a Data Controller makes personal data public and is asked to erase, destroy, or anonymise it, the Data Controller is responsible for implementing the necessary technical measures and incurring the necessary costs to comply with the request, as well as contacting others, including any relevant Data Controllers, in order to obtain their responses to the request for deletion.

Exceptions to the right of erasure provided by the PDPA include:

- A conflict with freedom of expression and freedom of expressing opinion.
- Compliance with public interest purposes in the areas of public health, historical archives, or educational research and statistics, subject to sufficient protective measures to protect personal data.
- Establishing, exercising, complying with, or defending legal claims.
- Compliance with legal obligations.

A Data Controller's response time to a request is not defined. In the event that the Data Controller fails to react to the request for deletion, the PDPA gives Data Subjects the opportunity to file a complaint with the competent authorities.

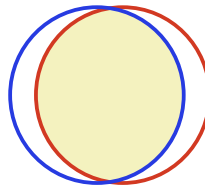
Notification(s) from the competent body pertaining to conditions on the deletion, which may include a specified timetable, may be issued in the future.

Unless specific restrictions apply, both the GDPR and the PDPA enable Data Subjects to request their personal information to be removed.

The GDPR and the PDPA have identical scopes and exemptions for the right to be forgotten. The key distinction is in the right's application, such as the types of requests and response times, which differ between these two pieces of law. Specification on the implementation of the right to be forgotten under the PDPA may be issued in the future.

Data Subjects' Rights

Criterion 16. Right to Object



85%

Similar

GDPR

Article 21

Data Subjects have the right to object to the processing of their personal data if:

- The processing of personal data is for direct marketing purposes, including profiling related to direct processing.
- The processing of personal data is for scientific, historical research, or statistical purposes, unless processing is necessary for the performance of a task of public interest.
- The processing is based on the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller, including profiling.
- The processing is based on the legitimate interest of the Data Controller or third parties, including profiling.

The Data Controller shall no longer process the personal data unless the Data Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.

A request to limit the processing of personal data must be replied to promptly, and in any case, within one month of receiving the request. Due to the complexity and amount of petitions, the deadline might be extended for another two months.

Section 32

PDPA

Data Subjects have the right to object to the processing of their personal data in the following situations:

- Personal data collected without consent as a result of tasks carried out in the public interest or based on a legitimate interest pursued by the Data Controller or a third party.
- Personal data processing for direct marketing purposes.
- Personal data processing for scientific, historical, or statistical research purposes.

A Data Controller can object to a Data Subject's request and continue to collect, use, and disclose their personal data on one of two grounds:

1. The Data Controller can demonstrate that the collection, use, and disclosure of personal data is based on a legitimate ground that outweighs the Data Subject's interests.
2. The Data Controller can demonstrate that the collection, use, and disclosure of personal data is for the purpose of establishing, exercising, or defending against a legal claim.

The PDPA does not state whether a Data Controller is required to provide Data Subjects with information on how to exercise their rights.

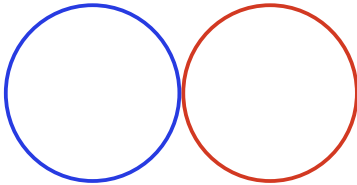
A Data Controller's response time to a request to limit the processing of personal data is not specified. In the event that the Data Controller fails to react to the request for objection, the Data Subjects have the right to file a complaint with a competent body.

Both the GDPR and the PDPA provide to Data Subjects the right to object to the processing of their personal data when such processing is carried out for direct marketing purposes, scientific, historical, or statistical research purposes, the performance of tasks of public interest or legitimate interest of the Data Controller or a third party.

The right provided by the GDPR is, however, more precise as the Data Controller must provide to the Data Subject information on how to exercise the right to object and reply to the Data Subject's request promptly, and in any case, within one month of receiving the request.

Data Subjects' Rights

Criterion 17.
Rights Related to Profiling



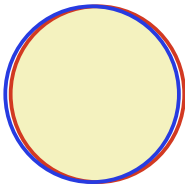
0%

Different

The right to profile is explicitly contained in the GDPR. The equivalent right does not seem to be contained in Thai law.


Data Subjects' Rights

Criterion 18.
Right to Restrict the Use of the Personal Data



98%

Similar




GDPR

Article 18

The Data Subject shall have the right to obtain from the Data Controller restriction of processing if:

- The accuracy of the personal data is contested by the Data Subject, for a period enabling the Data Controller to verify the accuracy of the personal data.
- The processing is unlawful and the Data Subject opposes the erasure of the personal data and requests the restriction of their use instead.
- The Data Controller no longer needs the personal data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims.
- The Data Subject has objected to processing pending the verification of whether the legitimate grounds of the Data Controller override those of the Data Subject.

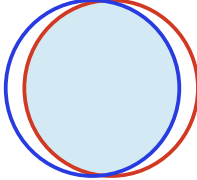
Section 34

PDPA 

The Data Subject may ask the Data Controller to restrict the collection of data when:


- The Data Controller is pending an examination process in accordance with the Data Subject's request.
- The Data Subject requests the restriction of the use of their personal data instead of its destruction or erasure.
- It is no longer necessary to retain the personal data for the purposes of its collection, but the Data Subject has necessity to request for further retention for the purposes of the establishment, compliance or exercise of legal claims, or defence of legal claims.
- The Data Controller is pending verification or pending examination in order to reject the objection request made by the Data Subject.

Whether it is the GDPR or the PDPA, the person concerned has the right to ask the Data Controller to restrict the use of their data (in accordance with the conditions required by the texts and in almost similar terms).

<p>Accountability Requirements</p> <p>Criterion 19. Appointment of a Representative</p>	 <p>90%</p>	<p>Similar</p>
---	---	-----------------------

 **GDPR** **Article 27, Recital 80**

Data Controllers and Data Processors not established in the EU (but that are subject to the GDPR) must appoint a representative in the EU, except if processing is occasional and does not involve large-scale processing of sensitive data.

Sections 37 (5), 38 **PDPA** 

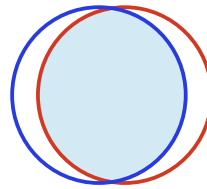
The Data Controller shall designate in writing a representative who must be in the Kingdom of Thailand and be authorised to act on behalf of the Data Controller without any limitation of liability with respect to the collection, use or disclosure of the personal data according to the purposes of the Data Controller.

The appointment of a representative is not required for public authorities and businesses that do not have a large amount of personal data.

Both the GDPR and the PDPA require Data Controllers that are not established in their territories to appoint a representative in writing in their territory.

Accountability Requirements

Criterion 20. Appointment of a Data Protection Officer



85%

Similar



GDPR

Articles 38, 39

Designation

Data Controllers and Data Processors, as well as their representatives, are obliged to designate a DPO under the GDPR, in any case where:

- The processing is carried out by a public authority or body, except for courts acting in their judicial capacity.
- The core activities of a Data Controller or Data Processor consist of processing operations that, by their nature, scope, and/or purposes, require regular and systematic monitoring of Data Subjects on a large scale.
- The core activities of the consortia consist of processing on a large scale sensitive data or personal data relating to criminal convictions and offences.

A group may nominate a single DPO who must be reachable by all establishments. When a public authority or body is the Data Controller or Data Processor, a single DPO might be appointed for many public authorities or bodies, depending on their organisational structure and size.

The DPO shall be designated on the basis of professional qualities, in particular expert knowledge of data protection law and practises.

Tasks and responsibilities

The DPO have at least the following tasks:

- To inform/advise the Data Controller or Data Processor and monitor compliance with their obligation under GDPR and other EU/national law applying to processing.
- To provide advice and monitor performance of Data Protection Impact Assessments (DPIA).
- To cooperate and act as a contact point with supervisory authorities.

Sections 41, 42

PDPA 

Designation

The PDPA requires Data Controllers and Data Processors, as well as their representatives, to designate a DPO in the following situations:

- The processing is carried out by a public authority or body.
- A Data Controller or Data Processor's activities relating to collection, use, or disclosure necessitate large-scale regular monitoring of personal data or the system.
- A Data Controller or Data Processor's core activities relate to the collection, use, or disclosure of specific categories of data.

In a supplementary notice of the PDPC, a list of public authorities or entities that need the appointment of a DPO will be expressly published.

A single DPO can be nominated as Data Controller and Data Processor when they are in the same affiliate business or in the same group of undertakings, as long as the DPO is freely accessible for all of them.

The DPO's appointment must be based on professional knowledge and competence in the field of personal data protection, as stipulated by the PDPC.

Tasks and responsibilities

The DPO's responsibilities include:

- Informing and advising the Data Controller, Data Processors, and their employees about their PDPA obligations.
- Monitoring the Data Controller or Data Processor performance, including their employees or service providers, with processing operations of the Data Controller, Data Processors, and their employees.
- Acting as a contact point for Data Controllers and Data Processors.

Position

The DPO must be involved in all issues relating to personal data protection, and must be provided all resources necessary to perform their tasks.

The DPO is independent and shall neither receive any instructions regarding the exercise of their tasks nor be dismissed or penalised for performing these tasks.

The DPO can fulfil other tasks and duties, but the Data Controller/Data Processor must verify that these tasks do not result in a conflict of interest.

Position

The DPO must be provided adequate tools and equipment to perform their tasks, and should be able to easily access the personal data.

The DPO's employment cannot be dismissed or terminated for the DPO's performance of their tasks and duties. When there is a problem related to the performance of their tasks, the DPO must be able to directly report to the chief executive of the Data Controller/Data Processor. The DPO can fulfil other tasks and duties as long as such tasks and duties are not against or contrary to the performance of their duties as a DPO.

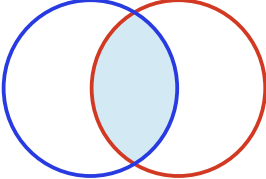
Data Controllers and Data Processors, or their representatives, are required under both the GDPR and the PDPA to appoint a Data Protection Officer (DPO). Both the GDPR and PDPA address the duties of the DPO.

Every public entity or organisation that processes personal data is required by GDPR to have a designated Data Protection Officer (DPO). A further PDPC announcement will detail the types of government agencies that call for the appointment of a DPO.

DPOs are considered independent under the GDPR. As far as we can see, the PDPA makes no overt statements on the autonomy of DPOs.

Accountability Requirements

Criterion 21.
Record of Processing



50%

Fairly Similar

Article 30, Recital 82

Data Controllers and Data Processors are required to keep a record of processing actions under their control. Furthermore, the GDPR establishes a list of data that a Data Controller must keep track of:

- The Data Controller's name and contact information.
- The purposes of the processing.
- A description of the categories of personal data.
- The categories of recipients to whom the personal data will be disclosed.
- The estimated time for erasure of the categories of data.
- A general description of the technical and organisational security measures used.

The GDPR also establishes a similar list for Data Processors, mandates that records be kept in writing or electronically, and specifies exceptions for businesses with fewer than 250 employees, unless the processing is likely to jeopardise Data Subjects' rights and freedoms, is not routine, or involves special categories of data.

Section 39

The Data Controller shall maintain the records in a written or electronic form, in order to enable the Data Subject and the Office to check upon.

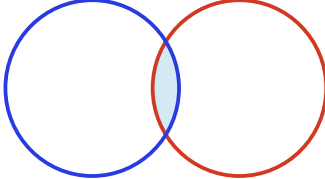
Records must contain at least:

- The collected personal data.
- The purpose of the collection of personal data in each category.
- Details of the Data Controller.
- The retention period of the personal data.
- Rights and methods for access to the personal data, including the conditions regarding the person having the right to access the personal data and the conditions to access such personal data.
- The use or disclosure of personal data without the consent of the Data Subject.
- The rejection of request or objection of the Data Subject's rights to access, to rectification, to erasure and right of portability.
- An explanation of the appropriate security measures.

A sub regulation has been under a Notification ("SME Notification") which provides relief from the requirement to prepare a record of processing activities ("ROPA") of the PDPA for Data Controllers that qualify as small and medium-sized enterprises ("SMEs") as defined under the Small and Medium-sized Enterprise Promotions Act ("SMEs Act").

Both the GDPR and the PDPA require Data Controllers and Data Processors to maintain records of their processing actions, and specify the data that shall be recorded. Through a recent Notification passed on 20 June 2022, under the PDPA, Data Controllers that qualify as small and medium-sized enterprises are exempted from keeping a record of processing activities.

Contrary to the GDPR, in the PDPA the Data Subjects can check on processing records.

<p>Accountability Requirements</p> <p>Criterion 22. Data Protection Impact Assessment (DPIA)</p>	 <p>15%</p>	<p>Different</p>
--	---	-------------------------

 **GDPR** **Article 35**


The GDPR requires Data Controllers to carry out a DPIA, in particular using new technologies, when the processing is likely to result in a high risk to the rights and freedoms of natural persons.

A DPIA is particularly required in the following situations:

- 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.
- Processing on a large scale of sensitive data.
- Systematic monitoring of a publicly accessible area on large scale.

At the very least, the evaluation must include the following:

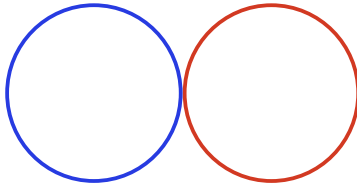
- A systematic description of the proposed processing operations and lawful processing purposes.
- The need and proportionality of the operations in connection to the purposes.
- Risks to Data Subjects' rights and freedoms.

Sections 37, 39, 40 **PDPA** 

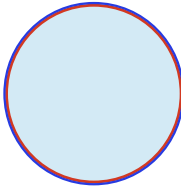
The PDPA does not require Data Controllers to conduct a DPIA *per se*. However, as part of their security obligations, Data Controllers must review their security measures when necessary or when the technology has changed.

DPIAs are particularly required under the GDPR in certain instances.

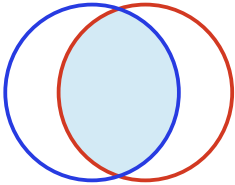
Although the PDPA does not mention DPIAs directly, it does state that Data Controllers must provide sufficient security measures and assess them as needed or when technology changes in order to successfully maintain suitable security and safety requirements. The Data Processor has a duty to provide appropriate security measures for personal data.

Accountability Requirements		0% Different
Criterion 23. Privacy by Design		

Contrary to the GDPR, the PDPA does not explicitly provide privacy by design principles. However, the Data Controller and the Data Processor are bound to provide appropriate security measures in order to prevent data breach incidents, which can be done through the implementation of privacy by design.

Accountability Requirements		100% Similar
Criterion 24. Audit Requirements		


Neither the GDPR nor the PDPA provide audit requirements.

<p>Accountability Requirements</p> <p>Criterion 25. Appointment of Processors</p>	 <p>70%</p>	<p>Fairly Similar</p>
---	---	------------------------------

 **GDPR**
Article 28

Where processing is to be carried out on behalf of a Data Controller, the Data Controller shall use only Data Processors that provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the Data Subject.

The Data Processor shall not engage with another Data Processor without prior specific or general written authorisation of the Data Controller. In the case of general written authorisation, the Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of other Data Processors, thereby giving the Data Controller the opportunity to object to such changes.

Section 40
PDPA 

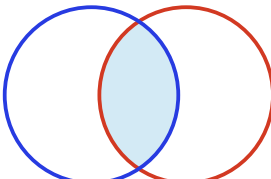
Where processing is to be carried out on behalf of a Data Controller, the Data Controller shall prepare an agreement with the Data Processor, in order to control that the activities of the Data Processor are carried out in compliance with the PDPA.

Both the GDPR and the PDPA require due diligence from the Data Controller in their relations with the Data Processor. In particular, both laws provide that the Data Controller is responsible for supervising the Data Processor's compliance or ability to comply with their provisions.

Contrary to the PDPA, the GDPR also provides that the Data Processor shall not engage a sub-processor without written authorisation from the Data Controller.

Accountability Requirements

Criterion 26.
Information Security



45%

Fairly Different

Article 32

Data Controllers and Data Processors are required to implement appropriate technical and organisational measures to protect the security of personal data, taking into account:

- The state of the art.
- The cost of implementation.
- The nature, scope, context and purpose of processing.
- The risk for the rights and freedoms of natural persons (depending on their likelihood and severity).

Security measures include:

- Pseudonymisation and encryption.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Sections 37, 40

PDPA

Data Controllers and Data Processors are required to provide appropriate security measures for preventing loss, access to, use, alteration, correction or disclosure of personal data. Appropriate security measures are required be in accordance with the minimum standard specified by the PDPC.

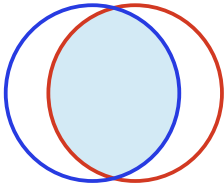
In this respect, in a Notification that came into force on 21 June 2022, the PDPC states that the Data Controller must require their Data Processor to provide the proper safeguard measures. As such, requirements under this Notification are applicable to both personal data Data Controllers and Data Processors.

Both the GDPR and the PDPA require Data Controllers and Data Processors to implement appropriate security measures in order to prevent data breaches.

The GDPR is more specific as it specifies which criteria are to be considered by the Data Controller or the Data Processor when they decide what security measures are appropriate.

The PDPA requires Data Controllers to comply with minimum standards issued by the PDPC. Such standards could be similar to the minimum security standards published by the Thailand’s Ministry of Digital Economy and Society, which, according to Tilleke & Gibbins, are similar to the ISO/IEC:27001 standard.

Also, the Notification (the “Notification on Security and Safeguard Measures”) dated 21 June 2022 under the PDPA, sets the minimum security measures for Data Controllers in processing personal data. Similarly to the GDPR, the required security measures consist of three key elements: confidentiality, integrity, and availability of personal data.

Accountability Requirements Criterion 27. Breach Notification	 75%	Similar
--	---	---

GDPR

Articles 33, 34

The GDPR requires the Data Controller to inform without undue delay (and when feasible not later than 72 hours after becoming aware of the breach) the appropriate supervisory authority in the event of a data breach, unless the personal data breach is unlikely to pose a danger to the Data Subject. The Data Processor must notify the Data Controller without undue delay after becoming aware of a personal breach.

When a personal data breach is likely to result in a high risk, the Data Controller must inform the Data Subjects implicated as soon as possible.

The notification must include at a minimum:

- A description of the nature of the breach, including, where possible, the categories and approximate numbers of Data Subjects affected, as well as the categories and approximate numbers of personal data records affected.
- The DPO or another contact point’s contact details.
- The likely consequences of the breach.
- Measures taken or proposed to mitigate the possible adverse effects.
- The reason for the breach.

Sections 37, 40

PDPA

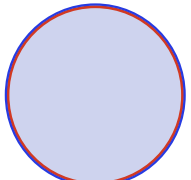
The PDPA requires Data Controllers to notify the Office of any personal data breach without delay (and when feasible, not later than 72 hours after becoming aware of it), unless such data breach is unlikely to result in a risk to the rights and freedoms of the person. The Data Processor is required to notify the Data Controller when a data breach has occurred.

When a personal data breach is likely to result in a high risk to the rights and freedoms of the Data Subject, the Data Controller must notify the breach and the remedial measures to the Data Subject without delay.

Further rules specifying how the notification must be executed shall be issued by the PDPC.

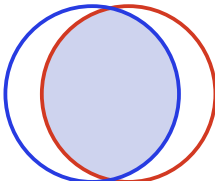
In both regulations, the Data Controller has to notify the authority without delay and as soon as possible and not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The GDPR directly specifies the elements that the notification shall include, while the PDPA refers to further rules and procedures set forth by the PDPC.


<p>Data Localisation and Transfer</p>	 <p>100%</p>	<p>Similar</p>
--	--	-----------------------


Criterion 28.
Data Localisation Requirements

Neither the PDPA nor the GDPR explicitly mention data localisation requirements.

<p>Data Localisation and Transfer</p>	 <p>75%</p>	<p>Similar</p>
--	---	-----------------------

Criterion 29.
International Data Transfer

 **GDPR** **Articles 5, 44-50**

Sections 28, 29 **PDPA** 

The GDPR enables personal data to be transferred to a third country or international organisation that meets the EU Commission’s criteria for adequate data protection.

In the absence of an EU Commission’s adequacy decision, transfers to third countries or international organisations are allowed if it is based on binding appropriate safeguards, including binding corporate rules.

In the absence of an EU Commission’s adequacy decision and binding appropriate safeguards, the transfer is authorised, by derogation, in the following cases:

- The Data Subject has explicitly consented to the transfer after having understood the risk of such transfer due to insufficient safeguards.
- The transfer is necessary for the performance of a valid contract between the Data Subject and the Data Controller.
- The transfer is necessary for the conclusion or performance by the Data Controller and other persons of a valid contract that is in the interest of Data Subject.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for establishment, exercise or defence of legal claims.

The PDPA establishes that personal data may only be transferred to a foreign country, where the destination country or international organisation has adequate protection standards, and is carried out in accordance with the principles set out by the PDPC.

In the absence of a decision from the PDPC, Data Controllers and Data Processors can transfer personal data:

- Where it is for compliance with the law.
- Where the consent of the Data Subject has been obtained, provided that they have been informed of the inadequate personal data protection standards of the destination country or international organisation.
- Where it is necessary for the performance of a contract to which the Data Subject is a party, or in order to take steps at the request of the Data Subject prior to entering into a contract.
- Where it is for compliance with a contract between the Data Controller, and other persons or juristic persons for the interests of the Data Subject.
- Where it is to prevent or suppress a danger to the life, body, or health of the Data Subject or other Persons, when the Data Subject is incapable of giving the consent at such time.
- Where it is necessary for carrying out the activities in relation to substantial public interest.

- The transfer is necessary to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent.
- The transfer (only to the extent laid down by the law) is made from a register which according to the law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest.

The transfer is also authorised in an *ad hoc* way if it is not repetitive, concerns a limited number of persons and is necessary for the purposes of compelling legitimate interests pursued by the Data Controller which are not overridden by the interest, rights and freedoms of Data Subjects.

A Data Controller or Data Processor located in Thailand can put in place a personal data protection policy regarding the sending or transferring of personal data to another Data Controller or Data Processor located outside of Thailand that is in the same affiliated business or in the same group of undertakings, in order to jointly operate the business or group of undertakings. When such a policy is reviewed and certified by the Office of the PDPC, transfers in accordance with the policy are exempt from a decision from the PDPC.

In the absence of a decision of the PDPC or personal data protection policy certified by the PDPC, Data Controllers and Data Processors can transfer personal data outside of Thailand if they provide suitable measures which enable the enforcement of the Data Subject's rights, including legal remedial measures according to the rules and methods prescribed by the PDPC.

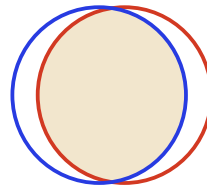
Both the GDPR and the PDPA rely mainly on adequacy decisions certifying that personal data is adequately protected in the foreign country.

The GDPR provides appropriate safeguards as a legal basis for third-country transfers which includes standard contractual clauses and binding corporate rules. The PDPA does not provide such a legal basis, it provides transfer authorisations that are similar to those. Similarly to binding corporate rules, Data Controllers and Data Processors can transfer personal data outside of Thailand to a Data Controller or Data Processor in the same affiliated business or group of undertakings when the transfer is in accordance with a data protection policy that has been certified by the Office. Similar to standard contractual clauses, Data Controllers and Data Processors can transfer data outside Thailand if they provide suitable measures enabling the enforcement of Data Subjects' rights according to rules and methods prescribed by the PDPC.

Both the GDPR and the PDPA provide exemptions from adequacy decisions and appropriate safeguards when the transfer relies on the Data Subject's consent, on a contractual basis, on the necessity to protect one's vital interests and on substantial public interests. Contrary to the PDPA, the GDPR also provides exemptions when the processing is necessary for establishment, exercise or defence of legal claims and when the data was available on a publicly available register. Contrary to the GDPR, the PDPA provides exemptions when the processing is necessary to comply with the law.

Enforcement

Criterion 30. Data Protection Authority



87.5%

Similar

GDPR

Articles 31, 51-59

The supervisory authorities have the jurisdiction to:

- Require the Data Controller or Data Processor to bring processing activities into accordance with the GDPR's rules, when applicable, in a particular way and within a set term.
- Apply a temporary or permanent restriction, such as a processing prohibition.

In accordance with EU or Member State procedural law, the supervisory authorities have the authority to:

- Order the Data Controller and Data Processor to provide any information required for the performance of their tasks.
- Obtain access to any premises of the Data Controller and Data Processor, including any data processing equipment and means.

The supervisory authorities also have the jurisdiction to reprimand and give warnings, and to require the correction or deletion of personal data, and apply administrative penalties.

The supervisory authorities have investigative rights, including the ability to conduct data protection audits, evaluate issued certificates, and alert the Data Controller or Data Processor of a suspected GDPR violation.

The GDPR explicitly states that each supervisory authority must carry out its responsibilities and wield its powers independently.

The GDPR is silent on the source of funds that must be made available to regulatory bodies. In this case, the Member State has complete choice over the source of financing.

Sections 8, 16, 18, 54, 72, 90

PDPA 

The PDPC has the duty to:

- Write the master plan on the operation for the promotion and protection of personal data.
- Promote and support government agencies and the private sector in carrying out of activities in accordance with the master plan, as well as to conduct the evaluation of the resulting operation.
- Determine measures or guidelines of the operation in relation to personal data protection.
- Issue Notifications or rules for the execution of the PDPA.
- Announce and establish criteria for providing protection of personal data which is sent or transferred to a foreign country.
- Announce and establish guidance for the protection of personal data as guidelines that the Data Controller and Data Processor are required to comply with.
- Recommend that the Cabinet enact or revise the existing laws or rules applicable to the protection of Personal Data.
- Recommend that the Cabinet enact the Royal Decree or reconsider the suitability of the PDPA at least every five years.
- Provide advice or consultancy on any operation for the protection of personal data of the government agency and private agency, in order to act in compliance with the PDPA.
- Interpret and render rulings with respect to the issues arising from the enforcement of the PDPA.
- Promote and support learning skills and understanding on the protection of personal data among the public.
- Promote and support research for the development of technology relating to the protection of personal data.
- Perform any other acts as prescribed by this Act, or other laws, which state the duties and power of the PDPC.

The expert committee(s) are appointed by the PDPC based upon their field of expertise and have the following duties and power:

- Consider complaints under the PDPA.

- Investigate any act of the Data Controller or the Data Processor that causes damage to the Data Subject.
- Settle disputes in connection with personal data.
- Carry out any other acts which are stipulated as the expert committee's duty and power under this Act or as assigned by the PDPC.

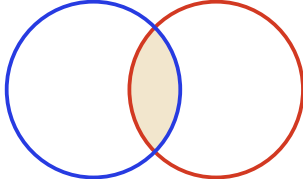
The PDPA states that the expert committee(s) may issue a warning before imposing a fine, and that the expert committee(s) shall consider the severity of the circumstances of the offence, the size of the organisation, and any other circumstances prescribed by the PDPC when deciding whether to issue an order to impose an administrative fine.

The PDPA is silent on whether a regulatory body must operate in total independence while carrying out its responsibilities.

The PDPA provides that the government and subsidies of national and international public entities, international governmental organisations, including interests, income earned from regulated authorities' property, are the sources of financing for regulatory authorities' operations.

Both the GDPR and the PDPA provide supervisory authorities with investigatory powers and corrective powers. Both laws have supervisory authorities that can require Data Controllers and Data Processors to comply with personal data protection law, apply temporary restrictions on data protection processing, require the Data Controller or Data Processor to provide any information or documents, enter the premises of the Data Controller or Data Processor, or issue warnings, reprimands and fines.

In the EU, each supervisory authority generally monitors one Member State's compliance (with the exception of Germany). In Thailand, according to the Data Protection Officer, Mr Montri Stapornkul, it is not clear yet how the expert committees will be divided.

Enforcement		Fairly Different
Criterion 31. Penalties		30%

GDPR

Article 83

Supervisory bodies may issue rules that include additional factors for calculating the monetary penalty amount. The GDPR allows for sanctions to be imposed on government entities. The creation of laws for the application of administrative fines to public agencies and organisations is left to Member States.

Depending on the infraction, the penalty may be:

- Up to 2% of worldwide annual revenue or €10 million, whichever is greater.
- 4% of global annual turnover or €20 million, whichever is greater.

Chapter VII - Part II
Administrative Liability

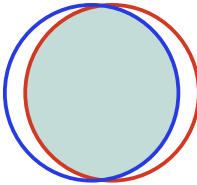
The amount of the penalty varies according to the nature of the violation of the law.


Non-compliance can be punished with administrative fines up to ฿5,000,000 plus punitive compensation.

The criteria used to set the administrative penalty are set out in a Notification in force from 21 June 2022, and include the severity of the violation, amount of damages, compensation paid to a Data Subject, standard of responsibilities of the Data Controller at the time of the violation, and business size of the Data Controller or Data Processor.


Certain breaches involving sensitive personal data and unauthorised disclosure are additionally punishable by up to a year in jail.

In both cases, the amount of the penalty varies according to the seriousness of the violation of the law. However, GDPR non-compliance fines are higher as they may be up to €20 million or 4% of the global annual turnover. The PDPA penalties can be up to ฿5 million (~ €134,400 using the currency rate on 30 March 2022). The Notification (“In the Notification on Administrative Penalties”) relates to the enforcement of penalties and how a Data Controller or Data Processor may be subject to administrative fines under the PDPA, depending on the severity of the violation. In the Notification, infractions are categorised as either “serious” or “non serious”.

Exemptions	 87.5%	Similar
Criterion 32. Anonymised Data		

 **GDPR** **Recital 26**

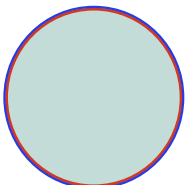
The GDPR does not apply to data that has been “anonymised”, meaning that it can no longer be used to identify the Data Subject.

Section 33 **PDPA** 

There is no mention of the applicability of the law to anonymised data.

Section 33 (4) only mentions that “The PDPC may announce the rules for the erasure or destruction of personal data, or anonymization of the personal data to become the anonymous data which cannot identify the Data Subject pursuant to paragraph one”.

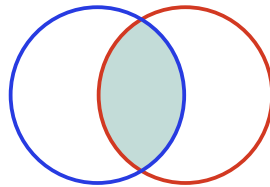
Neither the GDPR nor the PDPA apply to anonymised data.

Exemptions	 100%	Similar
Criterion 33. Social Media Intermediaries and Identity Management		

Neither the GDPR nor the PDPA mention the criterion “Social Media Intermediaries and Identity Management”.

Exemptions

Criterion 34. Exemptions for Research



50%

Fairly Similar



Articles 5, 9, 14, 17, 89
Recitals 33, 156, 159-161

Personal data processing for research purposes is governed by specific standards under the GDPR.

Processing of sensitive data is not prohibited under the GDPR when it is “necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, which shall be proportionate to the goal pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and interests of the Data Subject”.

According to the GDPR, special categories of personal data that require extra protection should only be processed for health-related purposes when absolutely necessary to achieve goals for the benefit of natural persons and society as a whole, such as in the context of public health studies.

The GDPR states that the processing of personal data for scientific research objectives should be construed “in a comprehensive way,” including “technological development and demonstration, basic research, applied research, and privately sponsored research”, among other things.

Under the GDPR, Member States may derogate from some Data Subjects’ rights, such as the right to access, the right to rectification, the right to object, and the right to restrict processing, if such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the achievement of those purposes.

Sections 25, 26, 32



In the PDPA, scientific, historical or statistical research purposes are a legal basis that allows the processing of personal data without consent and allows the processing of sensitive data.

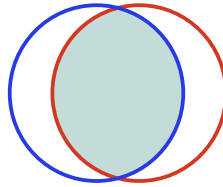
The PDPA also provides that scientific, historical or statistical research is subject to the exercise by Data Subjects of their right to object the processing, unless the processing is necessary to perform a task carried out for reasons of public interest by the Data Controller.

Both the GDPR and the PDPA authorise the processing of sensitive data for research purposes, as long as sufficient safeguards have been implemented to protect the Data Subjects’ basic rights and interests. Both the GDPR and the PDPA provide Data Subjects the right to object to processing unless the processing is necessary for the purposes of the public interest.

Contrary to the PDPA, the GDPR has special provisions derogating from some Data Subjects’ rights when such rights are likely to render impossible or seriously impair the achievement of specific purposes.


Exemptions

Criterion 35.
Application to Public Authorities




75%

Similar

 **GDPR** **Article 2**

The GDPR is not applicable to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Section 4 **PDPA** 

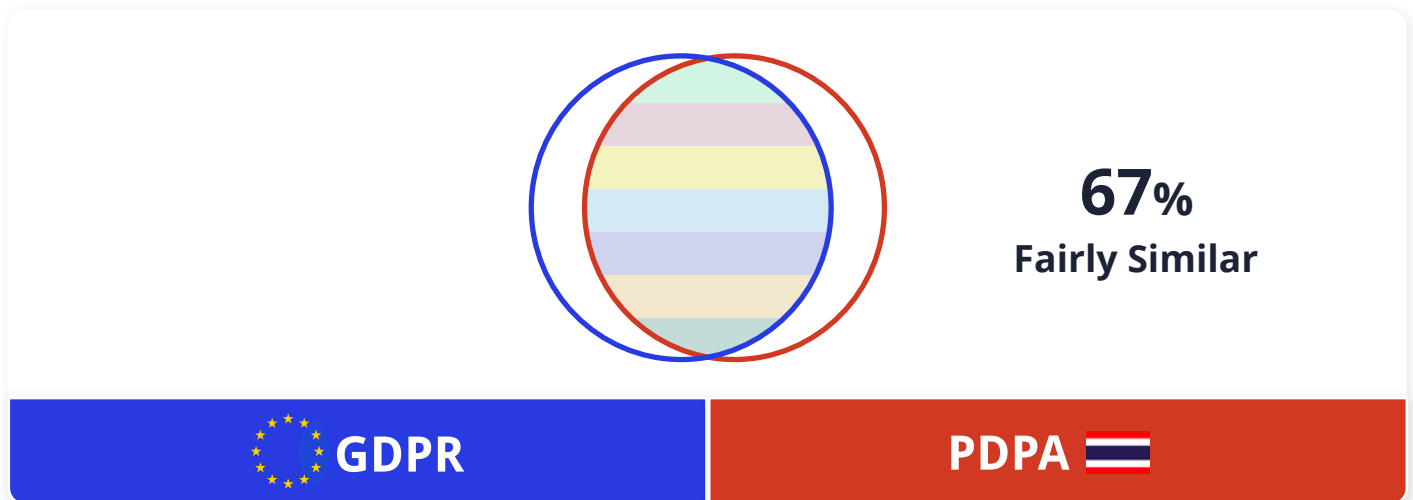
The PDPA is not applicable to the following public authorities:

- The operations of public authorities whose mission is to maintain the security of the State.
- The House of Representatives, the Senate and the Parliament (including committees appointed by the House of Representatives, the Senate or the Parliament), in the course of their duties and power.
- Court trials and judgements and the work operations of officers within the framework defined by the PDPA.

Both GDPR and PDPA are not applicable to law enforcement and judicial authorities.

The PDPA also exempts the House of Representatives, the Senate and the Parliament from its scope when they process personal data in the course of their duties and power.

Conclusion



The PDPA and the GDPR are fairly similar. A company doing business in the EU will definitely be familiar with most of the PDPA's provisions, and will be able to adjust its compliance program to PDPA's specific requirements. Our interview with Mr Montri Stapornkul, Thailand's Data Protection Officer, confirmed that the principles of the PDPA and the GDPR are quite similar, especially in terms of transparency, lawful use, and accountability.

Mr Stapornkul also stressed that companies doing business in Thailand must also be aware of the risk of facing criminal charges when they do not comply with some provisions of the PDPA. Additionally, Mr Stapornkul raised our awareness on the authority's power to shut down websites when their content is not neutral. Therefore, companies should carry out a global gap analysis that not only includes the PDPA's provisions, but also technology-oriented laws.

Designed to fill the legal vacuum in terms of personal data protection, the PDPA entered into force on 1 June 2022. Relating to the compliance of companies in Thailand, the professionals we interviewed shared the view that privacy is part of compliance and competition law. Therefore, compliance is expected to come through a domino effect, the compliance of one company triggering the compliance effort of its competitors.

However, according to the professionals we interviewed, the implementation of the PDPA is not easy because of the absence of guidelines. In May 2022, the Thai Board of Trade and the University of the Thai Chamber of Commerce carried out a PDPA readiness survey that revealed that only 8% of the 4,000 interviewed businesses had taken measures to be fully compliant with the law. The implementation of the PDPA is therefore a hot topic to follow, and businesses subject to the PDPA will have to be aware of the further legal developments that will be soon issued around the PDPA.

Compliance-as-Code: Our Solution

As this report highlights, there is a growing list of data protection compliance requirements around the world, with new laws and legislative requirements in place to assess how personal data or PII (Personal Identifiable Information) is being managed by companies.

Compliance is critical to every business: if you are not compliant with industry regulations, at best, you risk a fine and a bad reputation amongst your ecosystem and customers. At worst, you could be forced to shut your doors and stop trading completely.

At ALIAS, we work with companies and organisations of all sizes to help build in a compliance-as-code approach. Our APIs enable automated compliance: our PII Storage Duration API, for example, regularly assesses stored datasets to ensure that they meet regulatory requirements for the length of time data can be stored by a company.

By implementing compliance at the code level, you are able to automate regulatory prevention and monitoring, in order to increase your compliance coverage over time to 100%, with real-time feedback, and maintain oversight at 100%. This is what we call the DevRegOps approach.

In terms of Data Protection, what is Compliance-as-Code?

Data protection compliance-as-code refers to the tools and practices that allow you to embed the three core activities at the heart of compliance, at the code level of your organisation's tech stack:

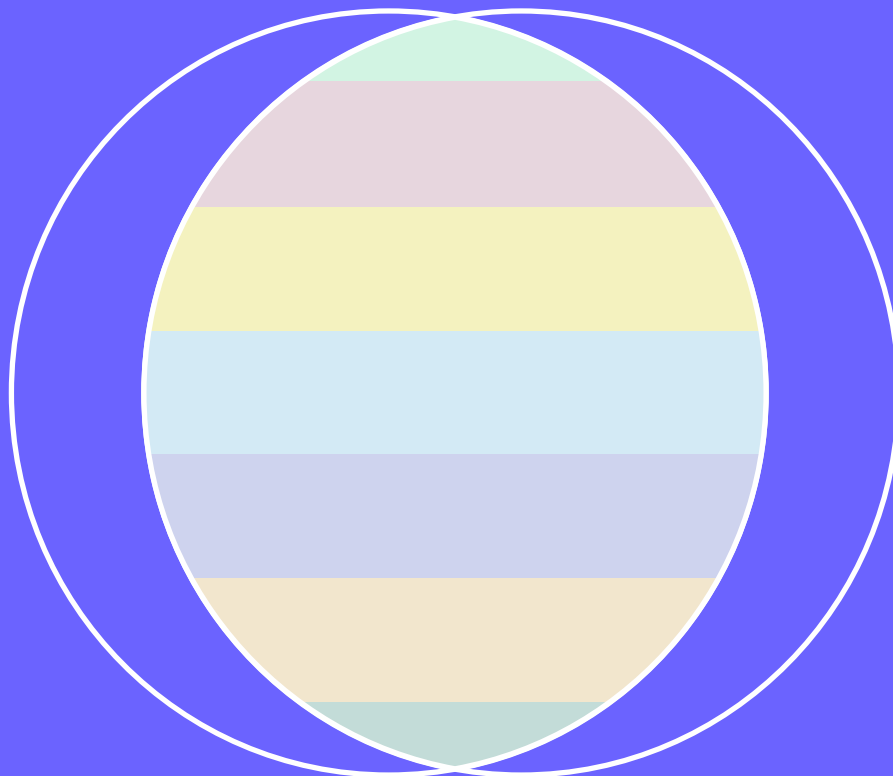
✓ Detect

✓ Solve

✓ Prevent

Contact us for a demo of our tools and to discuss implementing compliance-as-code solutions for your business.

Sign up to our [privacy newsletter](#) to receive information about changing legislations and news regarding data privacy protections.



www.gdpr.dev