Security and Compliance

Personal Data Protection Act Regulation Coverage

Version 2021.10.04

Table of Contents

Regulatory Obligations

On February 28th, 2019, the National Legislative Assembly approved the Thailand Personal data protection Act (PDPA). The act will pass into a law after it receives royal endorsement. The PDPA aims to govern data protection and will use GDPR as a blueprint, adopting some of the largest European articles to the Thai context.

Penalties

The PDPA imposes penalties for non-compliance. It is punishable with administrative fines (up to THB 5 million), criminal penalties (imprisonment up to one year and/or fines up to THB 1 million), and punitive damages up to twice the amount of the actual damages. Furthermore, civil damages under the PDPA can be multiplied as Thailand now allows data subjects to bring a class action lawsuit. The director of a company could also be subject to penalties under the PDPA.

The Mamori.io Difference

Mamori is a high performance all-in-one integrated security solution that makes it easy for any size team to secure, scale and monitor access to applications, APIs, servers and databases. The solution reduces the cost and technical expertise required to implement best practice security and data privacy for applications, APIs, databases and servers.

Mamori for IP (M4IP) protects all corporate resources from ransomware and unauthorized access.

Mamori for privileged access management (M4PAM) provides the technical safeguards, workflow automation and monitoring required to deliver both access and data privacy controls over ssh, sftp, rdp, and database access.

Mamori for applications (M4APP) provides the technical safeguards, workflow automation and monitoring required to deliver both access and data controls over http/s for REST, SOAP, and XML RPC interfaces.

Data Security Control

Category	Required Function	Details	Supported by mamori
Standard Options	Agent-less method	TCP, SSH, RDP, Database Authorization Proxy. No desktop or server agents required.	Yes
	Appliance type	Software appliance that run on commodity hardware. 4GB per 10000/queries/hour	Yes
	Installation without changes to network formation	Works with existing sub-nets. Gateway service allows unified access across difference networks.	Yes
	NIS-verified encryption modules	Verified modules by National Intelligence Service, such as INISAFE Crypto, are used	Yes
	No changes through installation	Even after installation, existing access methods can be used without changes of user's network set-ups or exclusive tools	Yes
	Transparent function	Transparently operates to network users and other equipment. Auditing and tracking are possible by users' real IP addresses	Yes
	Blocking bypass access	Users bypass connection paths are perfectly blocked by forming In-Line methods. SQL Firewall functions are offered. Policies combined white lists and black lists are used	Yes
	Support all common tools	Existing SSH,RDP, web and database connection tools can be used without using exclusive connection programs.	Yes
Access Control	Integrate with directory provider	Ability to map directory identities to database credentials	Yes
	Multi-factor connections	Ability to enhance logins with multi-factor support via standard DB tools	Yes
	Access control by IP / netmask	An access control policy by IP, IP,IP-port combination or netmask is offered	Yes
	Access control by time	An access control policy by periods, time, and date is offered	Yes
	Access control by SQL commands	Functions to allow and/or block specific SQL commands are offered	Yes
	Access control by executable	Functions to allow and/or block specific executable are offered	Yes
	Access control by role	Functions to allow and/or block specific roles are offered	Yes
	Session recording	Ability to record all session SQL	Yes
	Access control by tables	Functions to allow and/or block specific tables are offered	Yes
	Access control by columns	Functions to allow and/or block specific columns are offered	Yes
	Access control by rows	Functions to allow and/or block specific rows are offered	Yes
	Temporary elevated permissions	Functions to provide access and specific command permissions to systems, tables, columns, rows for a specified amount of time	Yes
	Alert on access events	Ability to notify via email, mobile IM service, or HTTP request	Yes
Data Control	Publishing Data Layer	Ability to provide access to virtual views that display data that is federated data from all systems	Yes
	Encryption	Access to a symmetric / asymmetric encryption key management system	Yes
	Dynamic data masking	Masking functions for securing important private information are offered	Yes
	Access control by columns	Functions to allow and/or block specific columns are offered	Yes

	Access control by rows	Functions to allow and/or block specific rows are offered	Yes
	Multiple policies per table	Functions to allow multiple policies per table	Yes
Log	Statistics	Statistics about users, administrator access, management, approval, access control, dormant accounts, and session control is offered.	Yes
	Reports	Reports about statistics is offered	Yes
	Monitoring	Session and/or authentication monitoring: real-time access, session changes, accessed object lists	Yes
		Monitoring about access control and/or contravention of policies	Yes
		Monitoring of policy requests, approvals, and execution	Yes
	Integration	Ability to integrate with log analytic solutions via API or SQL	Yes

Policy Coverage Summary

Mamori.io Is the most comprehensive data and database security solution in the market. The coverage table below lists all the GDPR and PDPA regulations that Mamori.io helps support.

Compliance Coverage				
GDPR		PDPA		
Article #	Article Name	Article#	Article Name	Mamori
5	Processing of Personal Data	26,37(2)	เก็บรวบรวมข้อมูลส่วนบุคคล	✓
6	Lawfulness of Processing			✓
7	Conditions for Consent			✓
8	Conditions of Child's Consent			✓
9	Processing Special categories	26	เก็บรวบรวมข้อมูลส่วนบุคคล	✓
10	Processing of Criminal Records	26	เก็บรวบรวมข้อมูลส่วนบุคคล	✓
15	Right of Access	30	สิทธิขอเข้าถึงข้อมูล	✓
17	Right to be Forgotten	33	สิทธิการลบข้อมูล	✓
18	Restriction of processing	34	สิทธิการระงับใช้ข้อมูล	✓
19	Notification obligation regarding rectification or erasure of personal data or restriction of processing			✓
20	Right to Data Portability	31	สิทธิในการเคลื่อนย้ายข้อมูล	✓
21	Right to Object	32	สิทธิโต้แย้งคัดค้าน	✓
22	Automated individual decision-making, including profiling			✓
25	Data Protection by Design & Default	37(1)	จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม	✓
30	Records of Processing Activities	40(3), 37(3)	จัดทำและเก็บรักษาบันทึกรายการของกิจกรรม	✓
32	Security of Processing	40(2)	จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม	✓
33	Notification of Data Breach	37(4)	แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	✓

Feature Comparison

	Mamori	Other Data Encryption & Control Solutions	Activity Monitoring Solutions
Comprehensive zero-trust Identify & Account Management	✓	✗	✗
Policy based rules to block, alert, report on any connection property, SQL statement, system access request, and privilege elevation.	✓	✗	Partial
Centrally managed Policy execution approval management	✓	✗	✗
Centrally managed per-session recording, auditing and monitoring	✓	✗	Partial
Comprehensive RBAC over data. Ranging from the ability to create “published” data sets without providing access to data to specific table, column, row making and filtering rules.	✓	Partial	✗
Dynamic data policy that can encapsulate rules spanning across multi-systems, multiple related data sets. Data could consist of files, APIs, and databases.	✓	✗	✗
Centrally manage policy lifecycle, alerts, and reporting	✓	✓	✓
Masking and encryption key management	✓	✓	✗
Data Quality and rectification policy management & monitoring	✓	✗	✗
Right to forget, retention, and restriction of processing data policy that can issue statements across multiple systems and APIs	✓	Partial	✗
Integration via REST API, web sockets, and SQL like syntax	✓	Partial	Partial

Regulation Articles

Processing of Personal Data *(GDPR Art. 5)*

It is the obligation of the data controller to ensure that all processing of personal data is secure, audited, monitored, and operates with the appropriate controls over approval processes that alter the state of the personal data.

How Mamori.io Helps

- Mamori's zero-trust access control solution provides all the role-based access control (RBAC) & technical safeguards required for secure, audited, and monitored data processing.
- No specialist development or specialist configuration required
- Use any condition to mask, encrypt, and control processing of all or part of a data subjects' personal data across database systems and APIs
- Approval process for the request & execution of policy that control data processing permissions
- Monitor, alert, and block at all levels of data governance: connection, SQL session, and policy workflows.

Lawfulness of Processing & Consent *(GDPR Art. 6,7, & 8)*

Data controllers must obtain **consent** for personal information processing. These requests must be phrased clearly and not deceive or be misleading. Consent should be approved in writing or through electronic means unless it is impossible by its nature. Consent can be foregone in different situations such as in case of legitimate reasons, public interest or the performance of contractual obligations.

Once consent is obtained there must valid lawful basis in order to further process personal data. There are six available lawful bases for processing, and which basis is most appropriate depends on the purpose and relationship with the individual. Lawful processing depends on being "necessary" and not achievable though a different method with the data. Processing is not deemed necessary solely because the controller has chosen to operate the business in a particular way, but rather if whether the processing is objectively necessary for the stated purpose. All applicable lawful basis must be determined and document before processing.

The six lawful bases are: consent, contractual, legal obligation, vital interests, public task, and legitimate interests.

How Mamori Helps

- **On Policy Definition** - Mamori allows policy officers to specify the legal basis for each of the respective policy procedures that control the data processing of personal data.
- **On Data Requests** - Applicants requesting access to data under a specific policy can enter the legal basis or reason for the request. Approval officers can accept or deny the request and provide a reason for their decision. Both the applicant and policy officers are verified through zero-trust security access controls.
- **On Policy Execution** - The full lifecycle of the processing is logged: request, approval, policy execution, and data processing.
- **Monitoring and Reporting** - Data controllers and policy officers can receive alerts and monitor activity on any part of the policy data lifecycle.

Processing Special categories *(GDPR Art. 9)*

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited except for reasons (a) to (j) listed in Article 9 GDPR.

Processing of Criminal Records *(GDPR Art. 10)*

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 official authority.

How Mamori Helps with GDPR Articles 9 and 10

- **On Access** - All users that access data are verified using zero-trust authentication
- **On Policy Definition** - Mamori can mask and encrypt special category and criminal data in motion or at rest. Allowing policy controllers to create the required policies and roles that enable the control and administration of the data policy.
- **On Data Requests** - Applicants requesting access to special category data are required to enter the reason for the request. Approval officers can accept or deny the request and provide a reason for their decision. Both the applicant and policy officers are verified through zero-trust security access controls.
- **On Policy Execution** - The full lifecycle of the processing is logged: request, approval, policy execution, and data processing.
- **Monitoring and Reporting** - All data access is logged and monitored. Data controllers, administrators, and policy officers can receive alerts and monitor activity on any part of the data processing lifecycle.

Right of Access *(GDPR Art. 15)*

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing & the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; where possible, 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 from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- where the personal data are not collected from the data subject, any available information as to their source;

- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

How Mamori Helps

Mamori provides the data controller much of the technical required evidence and policy data to meet a "Right of Access" request from a data subject:

- The data processing policies that reference the personal data
- The systems, role types and external identities that have processed the personal data.
- Status of request initiated by the data subject:
  - Restriction of processing
  - Right to be forgotten
  - Rectification
  - Portability

Right to be Forgotten *(GDPR Art. 17)*

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay.

How Mamori Helps

- **On Policy Definition** - A single Mamori RTF policy procedure can implement logical and physical deletion across different database systems and application API. On the application level data can be logically redacted or filtered out. In the database level data can be archived to a different database, purged, masked and/or encrypt.
- **On RTF Requests** - Applicants can request the execution of deletion for a data subject. Approval officers can accept or deny the request and provide a reason for their decision. Both the applicant and policy officers are verified through zero-trust security access controls.
- **On Policy Execution** - The full lifecycle of the processing is logged: request, approval, policy execution, and data processing.
- **Monitoring and Reporting** - All right to forget processing is logged and monitored. Data controllers, administrators, and policy officers can receive alerts and monitor activity on any part of the right to forget (RTF) data processing lifecycle.

Restriction of processing *(GDPR Art. 18)* & Right to Object *(GDPR Art. 21)*

The data subject has the right to obtain from the controller **restriction of processing** (permanent or limited for a period of time) where one of the conditions listed in Article 18 applies.

The data subject shall have the **right to object**, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including automated profiling based on those provisions.

In either case the controller shall no longer process the personal data unless the 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.

How Mamori Helps

- **On Policy Definition** - A Mamori restriction or objection policy procedure can execute any number of methods to remove the specific personal data from processing either permanently or for a specified period of time. Examples of technical methods, but not limited to, are dynamic masking, filtering, and temporarily move data to another system.
- **On Requests** - Applicants can request the execution of restriction for a data subject. Approval officers can accept or deny the request and provide a reason for their decision. Both the applicant and policy officers are verified through zero-trust security access controls.
- **On Policy Execution** - The full lifecycle of the Restriction of Processing is logged.
- **Monitoring & Reporting -** All right to Restriction processing is logged and monitored. Data controllers, administrators, and policy officers can receive alerts and monitor activity on any part of the processing lifecycle

Notification obligation regarding rectification or erasure of personal data or restriction of processing (GDPR Art. 19)

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.

The controller shall inform the data subject about those recipients if the data subject requests it.

How Mamori Helps

- **On Policy Execution -** Policy procedures can be configured to call APIs that notify data subjects and also send mobile alerts and email notifications to policy agents and data controllers that a particular policy has been executed
- **Monitoring & Reporting -** Data controllers, administrators, and policy officers can review and extract all executed policies for a specified period of time and forward them for

notification processes.

Right to Data Portability (GRPD Art. 20)

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

How Mamori Helps

- **On Policy Definition -** Define policies and cross platform federated virtual business views that can be used to extract the data for the applicant.
- **On Execution -** All access and SQL executed is logged, and alerts and notifications to policy owners can be configured.
- **Monitoring & Reporting -** Data controllers, administrators, and policy officers can review all executed data extraction policies for a specified period of time.

Automated individual decision-making, including profiling *(GDPR Art. 22)*

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

How Mamori Helps

- **On Policy Definition** - A Mamori policy procedure can execute any number of methods to exclude specific personal data from AI processing either permanently or for a specified period of time. Examples of technical methods, but not limited to, are dynamic masking, filtering, and temporarily move data to another system.
- **On Requests** - Applicants can request the exclusion for a data subject. Approval officers can accept or deny the request and provide a reason for their decision. Both the applicant and policy officers are verified through zero-trust security access controls.
- **On Policy Execution** - The full lifecycle of the AI exclusion is recorded.
- **Monitoring & Reporting -** All exclusion processing is logged and monitored. Data controllers, administrators, and policy officers can receive alerts and monitor activity on any part of the processing lifecycle

Data Protection by Design & Default (GRPD Art. 25)

Companies/organisations are encouraged to implement technical and organisational measures, at the earliest stages of the design of the processing operations, in such a way that safeguards privacy and data protection principles right from the start ('data protection by design').

By default, companies/organisations should ensure that personal data is processed with the highest privacy protection (for example only the data necessary should be processed, short storage period, limited accessibility) so that by default personal data isn't made accessible to an indefinite number of persons ('data protection by default').

How Mamori Helps

Mamori is the only comprehensive data solution in the market that offers access controls, data controls, and PDPA policy workflow management.

- **For applications** - Full support for implementing in-line and out-of-band access controls, data controls, and PDPA policies.
- **For Business Intelligence & DevOps**- Implement zero-trust access controls, data controls, and PDPA policies for desktop analytics and ad-hoc SQL tools.
- **Monitoring & Reporting -** All SQL processing is logged and monitored. Data controllers, administrators, and policy officers can receive alerts, monitor activity, and create session policies to block unwanted statements.

Records of Processing Activities (GDPR Art. 30)

In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility and where possible, the envisaged time limits for erasure of the different categories of data.

Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

How Mamori Helps

- **On definition** - Mamori data retention policy procedures can be scheduled to execute and remove data from processing that has exceed the specified time limit.
- **Reporting -** Mamori provides data controllers a full audit history of access, session statement execution, policy requests, policy executions, and policy changes.

Security of Processing (GDPR Art. 32)

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

the pseudonymisation and encryption of personal data;

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.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

How Mamori Helps

Mamori is the only comprehensive data solution in the market that offers access controls, data controls, and PDPA policy workflow management.

- Mamori's zero-trust access control solution provides all the role based access control (RBAC) & technical safeguards required for secure, audited, and monitored data processing.
- No specialist development or specialist configuration required
- Use any condition to mask, encrypt, and control processing of all or part of a data subjects' personal data across database systems and APIs
- Approval process for the request & execution of policy that control data processing permissions
- Monitor, alert, and block at all levels of data governance: connection, SQL session, and policy workflows.

Notification of Data Breach (GDPR Art. 33)

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. 2Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

How Mamori Helps

In the case of a breach, Mamori's audit logs and anomaly alerts analytics can pinpoint exactly which data was exposed and breached, and shorten reporting time, while providing accurate

and accountable information.