How **Aspire Systems complies** with **Privacy laws**

aspire SYSTEMS
attention. always.

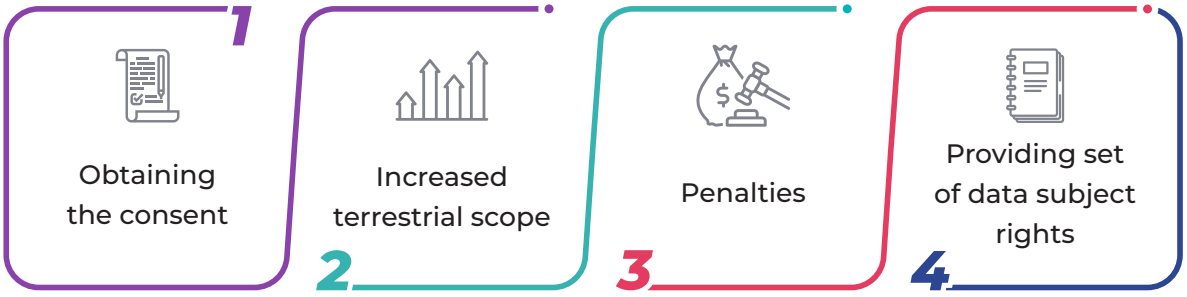
www.aspiresys.com

Table of Contents

How Aspire Systems complies with Privacy laws

Introduction

The key objective of the GDPR, CCPA and PDPA is to protect personal data of respective nationals and resident from data breaches and other manipulations that happens in this rapidly growing digital era. Though the directive on privacy was established in 1995, the key principles of data privacy are similar from the earlier directive(s), however the applicable privacy laws sets a new paradigm of protecting privacy of respective nationals and/or residents by imposing the following on the business that utilizes personal data:



The applicable privacy law requirements has made businesses to collect, process and store privacy data collected directly or indirectly more responsibly and to provide appropriate safeguards. In addition, the GDPR, CCPA and PDPA brings in more accountability to organization that handles personal data.

In this white paper, Aspire systems provides the overview of how the organization complies with GDPR, CCPA and PDPA in its capacity as a Data Controller as well as a Data Processor.

Key Definitions

The goal of becoming a risk guardian requires insurers to drive front-to-back modernization to help them address both growth and efficiency mandates. They need to build a modern core foundation and leverage a core technology partner ecosystem. To extract speed-to-market benefits and maximize value from their core systems, insurers should follow a three-pronged agenda:

ISO 27701	GDPR	CCPA	PDPA
PII Principal	Data Subject	Consumers	Individual
PII Processor	Data Processor	Service Provider	Data Intermediary
PII Controller	Data Controller	Buisiness	Organization
Joint PII Controller	Joint Data Controller	-	-

- PII Controller: Refers to a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the **processing of personal data.**

- PII Processor : A natural person or legal entity that processes personal data on behalf of Data Controller.

- PII Principal: Refers to a natural person who is the subject of personal data

Scope of Privacy in Aspire

The scope of the GDPR, CCPA and PDPA compliance in the organization in a broader sense applies to any personal data about applicable nationality (s) or resident(s) that is available with the organization. In case of Aspire, the scope also lies with its role both as PII controllers as well as PII processor. The locations in India such as Chennai and Hyderabad, Kochi, Bangalore act only as PII processors. The location at Poland, California, Singapore is both a PII controller and PII processor. The scope of processing of data is either by automated means or non–automated means.

Basic Principles of GDPR, CCPA and PDPA

As mentioned in GDPR, CCPA and PDPA following principles are adopted in the organization Personal data shall be:

1. **'Lawfulness,Fairness and Transparency' -** processed lawfully, fairly and in a transparent manner in relation to the data subject

2. **'Purpose Limitation' -** collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes

3. **'Data Minimization' -** adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. **'Accuracy' -** accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

5. **'Storage Limitation' -** kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject;

6. **'Integrity and Confidentiality' -** processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures

7. **Privacy by Design and Default:** This principle requires that privacy be incorporated into the design and operation of all information systems and processes.

8. **Storage Limitation:** Should only retain personal information for as long as necessary to fulfill their intended purpose, and should securely dispose of it when it is no longer needed

9. **Accountability:** Should be accountable for complying with applicable privacy laws and regulations and should establish processes for handling privacy-related complaints and inquiries.

Consent

The processing of data can begin only after an affirmative act or an explicit declaration provided by the PII Principal . Privacy laws defines consent as 'freely given, specific, informed and unambiguous indication of the PII Principal's agreement to the processing of personal data relating to him or her.'

☑ **I AGREE**

☒ **I DO NOT AGREE**

The consent form provides details on personal data that would be collected, how and where it will be processed, to whom it will be shared and where it will be stored. The consent form also highlights the PII Principal' rights on personal data handling as provided below

Rights of PII Principal

As per Applicable Privacy law, the PII Principal has the following rights. The organization complies with the rights with a defined response time lines

1. **Right to information -** Right to ask what personal data of theirs is processed and with whom it is shared

2. **Right to access -** Right to access their own data as well as request copies of the same

3. **Right to rectification -** Right to request for change to their data if it not accurate

4. **Right to withdraw consent -** Right to withdraw the previously given consent, so that company does not process their data anymore

5. **Right to object -** Right to object when his/her data is processed in variance to committed purposes. This is akin to 'Withdrawal of Consent'

6. **Right to object to automated processing -** Right to demand only manual processing to understand the uniqueness of the data subject

7. **Right to be forgotten -** Right to request for deletion of their data. To be in conjunction with retention period and retention schedule in-line with applicable laws

8. **Right for data portability -** Right to return the data or transfer it to another controller The timelines for the responding to data subject's request is as follows.

9. **Right to non-discrimination -** Right to non-discrimination cannot deny services, charge you a different price, or provide a different level or quality of services just because you exercised your rights under the CCPA.

10. **Right to limit -** Right to Limit can direct to only use your sensitive personal information for limited purposes, such as providing you with the services you requested.

11. **Right to make a compliant -** Right to Make complaint if they believe that their personal data has been mishandled by an organization.

GDPR TAT:

Data Subject's Request	Turn Around Time
The Right to be informed	1 Month
The Right to access	15 days
The Right to rectification	1 Month
Right to Withdraw consent	1 Month
Right to object to automated processing	1 Month
The Right to Erasure	15 days
The right for data portability	1 Month
The right for restriction	1 Month

CCPA TAT:

Data Subject's Request	Turn Around Time
The right to know	1 Month
The right to delete	15 days
The right to opt-out	1 Month
The right to non-discrimination	1 Month
The Right to Limit	1 Month
The Right to correct	1 Month

PDPA TAT:

Data Subject's Request	Turn Around Time
The right to access personal data	30 Days
The right to correct personal data	30 Days
The right to withdraw consent	30 Days
The right to limit the use of personal data	30 Days
The right to portability of personal data	30 Days
The right to object to the use of personal data	30 Days
The right to be informed of data breaches	No later than 72 hours after becoming aware of the breach.
The right to make a complaint to the Personal Data Protection Commission (PDPC)	30 Days

Responsibilities as PII Controller and Processor

As a PII Controller:

Aspire as a PII controller owns the complete accountability for the PII Principal Personal data that is obtained. It maintains the records of its processing activities and its associated consents. The list of records that would be maintained is provided as an annexure to this document. In case of engaging a third-party data processor, a formal data processing agreements (DPA) is established between Aspire Systems (PII Controller) and the PII processor (Third party). The PII processor safeguards are evaluated before data processing commences with the processer. In addition, periodic audit is conducted on the PII processor.

As a PII Processor:

In cases where Aspire systems act as a PII processor, its processing of personal data is in line with the data processing agreement with the PII controller. As a PII processor, Aspire systems shall not employ another processor without the controller's authorization.

Data Security Provisions:

The PII controllers are required to ensure the security of the data that is being processed or stored. Aspire provide security by design or default for all processing activities. The internal systems that are built with designs that meets the principle of data minimization (adequate, relevant and limited).Our privacy strategies such as privacy by design and default will mitigate the impact in case of a data breach.

At Aspire systems, the appropriate data security controls are formulated using data protection impact assessment (DPIA) of the personal data and its processing requirements. Security programs are designed to implement the data security controls identified. The security programs are guided using

1

Program Management activities

2

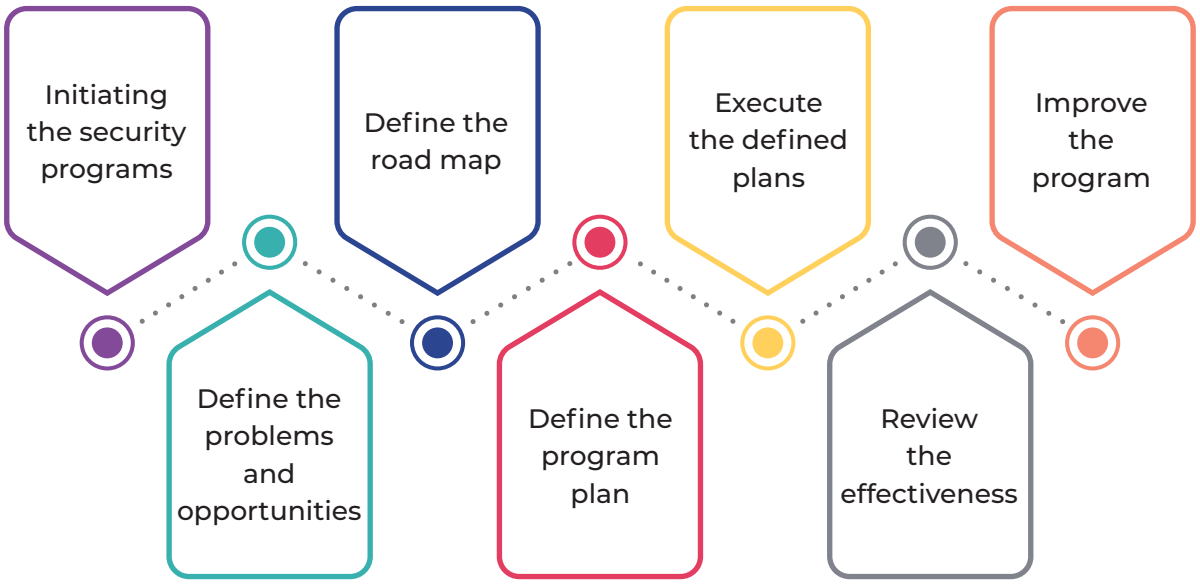
Process Management activities (Policies, Procedures, templates)

3

Tools and Services (Technology based Controls)

Program Management activities

The most important managerial function includes the following

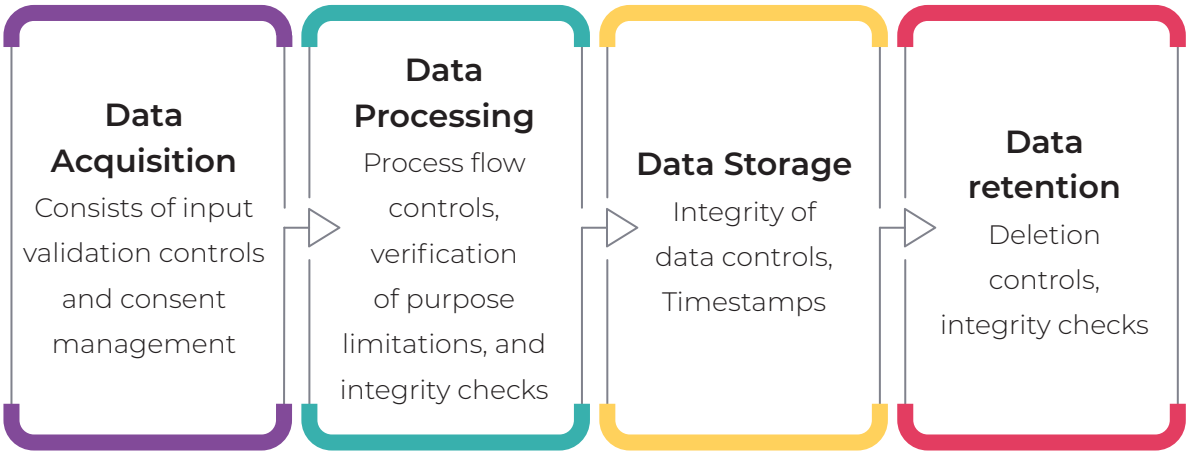


Process Management activities

The processes are defined in-line with the security programs defined. The security policies and associated procedures are formulated to meet the exact requirements of data protection and privacy controls. The policies such as privacy policies reflect the faith by which the organization takes cognizance of security parameters and ensures highest level of safeguards. The procedures extend the defined policies and formulate the implementation steps of the security controls. The policies and procedures are reviewed at least once every year or as when required.

Tools and Services

In order to meet the various requirements of GDPR CCPA and PDPA, Aspire systems expedites technology based controls using tool kits, software that are completely automated or partially automated. The goal is to minimize manual intervention unless sought byPII Principals. The Data Protection and Privacy (DPP) controls are part of the internal control systems. A typical DPP control sets are as follows



One of the key objectives of having tools is place is to maintain all key registers mandated in the digital form.

In case of Aspire being a PII processor, Aspire ensures the instructions from the data controller are adhered to.

Notification of Breach

In case of a security breach, as a data controller Aspire systems is obliged to report it to the supervisory authority and to the affected PII Principals within 72 hours and as a data processor , Aspire system is obliged to report it to the data controller in case of any data breach.. If the data breach is unlikely to result in the risk of data privacy of the PII Principals, then the same shall be tracked as an internal issue and no specific breach reports are submitted to supervisory authority and PII Principals.

Compensation and Liability

PII Principals have the right to receive compensation in case of data breach that affects their personal data. The amount of liability depends on the gravity of infringement and whether it was due to negligence or intentional and other key considerations. The risk of liability is mitigated by the ability to demonstrate the presence of key controls as per GDPR, CCPA and PDPA requirements.

For GDPR: The highest liability could be 4% of global turnover or 20 Million Euros whichever is greater.

For CCPA: Provides for civil penalties of up to $2,500 for each violation, and up to $7,500 for each intentional violation.

For PDPA: 1 million SGD or where the organization's annual turnover in Singapore exceeds SGD 10 million, 10% of the organization's Singapore turnover.

Conclusion

Aspire systems has implemented necessary security controls to meet the requirements of GDPR, CCPA and PDPA. This includes establishment of comprehensive policies and procedures, obtaining consent from data subjects, ensuring adequate security controls while processing and storing and honoring the commitment to PII Principal rights. Both as a PII controller and PII processor, Aspire systems complies with the various privacy laws(GDPR, CCPA and PDPA).

Authors

Documented by

Kavitha Ayappan

Thanks to the Reviewers

Sunil JNV, Aju Mathew,
Raghu Ragavan,
Binu john and Pawel Bejger

Thanks to Dr N R Mukundan from Rhythmtec for his valuable inputs and suggestions.

aspire SYSTEMS
attention. always.

Aspire Systems is a global technology services firm serving as a trusted technology partner for insurers worldwide. With 20+ years of experience in software product engineering, we understand the depth and breadth of Insurance Business. We work with some of the world's leading Insurance Providers, helping them leverage technology to become Future Ready. Our domain experts and certified professionals provide end-to-end solutions from discovery to support and maintenance. Our expertise and insurance software solutions in Digital Customer Experience, Operational Excellence, and Guidewire Transformation makes us the most preferred Insurtech transformation partner. Our core philosophy of "Attention. Always." communicates our belief in lavishing care and attention on our customer and employees.

For more info contact: info@aspiresys.com or visit www.aspiresys.com

USA	SINGAPORE	INDIA	BELGIUM
+ 1 630 368 0970	+65 3163 3050	+91 44 6740 4000	+ 32 3 204 1942

NETHERLANDS	POLAND	MEXICO
+ 31 (0)30 800 92 16	+48 58 732 77 71	+52 222 980 0115