A2024 ASEAN IPA
Annual General Meeting & Conference

# Understanding and Harmonization Data Privacy Regulations

March 2, 2024

Kozo Takeuchi
President Elect of APAA HQ

# Index

1. To share the speaker's perspective on current issues on Data Privacy matters
2. To share the speaker's perspective on the importance of establishment of regional data privacy frameworks
3. To share the speaker's forecast on the future of Data Privacy

# Data Privacy（1）

(1) What is data privacy ?

Data privacy refers to the right to decide when, how, and to what extent personal data is protected or controlled.

(2) What is personal data?

Personal data may include your name, location, contact information, and online and real-world activities. Data privacy is not personal data.

# What is Personal Data ?

| Personal Data | Industry Data | Public Data |
|---|---|---|
| ▪Basic Info（Name, Address, Birth, Sex, etc.)<br>▪Healthcare Data( Clinical history etc.)<br>▪Identification info (face, finger print etc.)<br>▪Vital data（Body temperature, Blood type, Blood pressure, Pulse rate etc.)<br>▪Emergency contact<br>▪Care recipient data | ▪Factory design information<br>▪Parts processing data<br>▪Product assembly data（Number of products and products in progress, etc.)<br>▪Environmental data（Ambient temperature, humidity, etc.)<br>▪Inspection information(material, product form, weight, etc.)<br>▪Human motion data<br>▪Image/Video data<br>▪Device/Equipment data (parameter, operating time,velocity, vibrancy, temperature, sound etc.)<br>▪Maintenance information | ▪Road/ Transportation Data<br>▪Weather/Disaster Information<br>▪Sightseeing Data<br>▪Map data<br>▪Immigration Data<br>▪Local Government Data<br>▪Public service information (electric, gas, water etc. )<br>▪Local government information (tax, insurance,election, events, facilities etc. ) |

# Data Privacy（2）

(3) Importance

With the spread of the Internet, the importance of data privacy is increasing. Websites, applications and social media platforms need to collect and store your personal data in order to provide their services.

(4) Function

Data Privacy Frameworks provide how data is collected, stored, and shared with third parties while protecting personal data.

# Regional Data Privacy frameworks（1）

(1) What is data privacy frameworks

Regional data privacy frameworks refer to a set of regulations and guidelines governing the protection and handling of personal data within a specific geographical area such as ASEAN and APEC or jurisdiction such as EU.

| ASEAN (personal data) | EU GDPR (personal data) | APEC (personal data) |
|---|---|---|

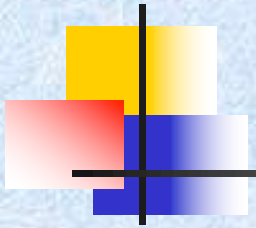
# Regional Data Privacy Frameworks（2）

（2）Purpose

ASEAN regional data privacy frameworks aim to protect individuals' privacy rights and regulate the processing of personal data, thus seeking to foster regional integration and cooperation and to propel ASEAN towards a secure, sustainable and transformative digitally-enabled economy, just like the European Union's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA),

However, these frameworks also face several challenges and problems..

# Regional Data Privacy Frameworks（3）



(3) Common frame work components

(i) Requirements for obtaining consent

(ii) Transparent data practices

(iii) Data breach notifications,

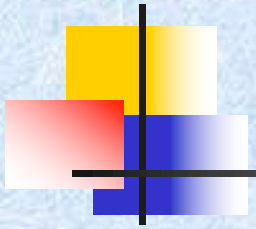
(iv) Establishment of component authorities to enforce compliance

# Comparison of Regional Data Privacy Frameworks

Regional Privacy Frameworks and Cross-Border Date Flows ( GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf)

| | ASEAN | APEC | EU GDPR |
|---|---|---|---|
| Objective | Economic | Economic | Fundamental rights |
| Application scope by jurisdiction | Territorial- subject to national law | Territorial- subject to national law | Extra-territorial- not subject to national law |
| Application scope by entity data controllers vs. processors | Data controllers | Data controllers +processors (voluntary) | Data controllers +processors (mandatory) |
| Accountability provisions | Principle | Principle + Voluntary mechanism | Principle + voluntary mechanisms + legal requirements |
| Consent requirements | Consent, where applicable | Consent, where applicable | Consent (freely given, specific, informed and unambiguous, and in some cases, explicit consent ) |
| Default position on data flaw-services to promote vs. restrict | Promotes data flow | Promotes data flow | Restrictive ( outside the group); promotes data flow (within the group) |

# Future of Data Privacy (1)



（1）Compliance Burden

Members may struggle to comply with multiple sets of regulations, each with its own requirements and penalties for non-compliance, leading to increased costs and administrative burdens.

Huge penalty cases due to violation of GDPR

-NTT Data Spain---64,000 euro

-Google—50 million euro

-Amazon---746 million euro

# Future of Data Privacy (2)

(2) Utilization and Protection

In recent years, data privacy has received increasing attention due to demands for measures to strengthen data protection laws and regulations, and the need for data utilization has also increased.

Therefore, there will be an increasing need to consider how to utilize data while protecting it and to review operational rules and systems in line with data privacy protection systems.

# Future of Data Privacy (3)

(3) Enhancement of data security

Personal data will be utilized while enhancing data security through various hacking prevention techniques such as encryption, tokenization, and hashing.

This is why "Privacy Enhancing Technologies" are attracting attention. This initiative, abbreviated as "PETs," is attracting attention as a technology that can perform highly accurate data analysis while protecting privacy, especially technologies such as "secure computation," "differential privacy," and "federated learning."

# Future of Data Privacy (4)

(4) Inconsistencies

Variances in regional data privacy laws can create inconsistencies in how data is protected and managed, potentially undermining the overall effectiveness of privacy measures.

(5) Cross-Border Data Transfers

Restrictions on cross-border data transfers can hinder global data flows, impacting international businesses, innovation, and economic growth.

# 7 Conclusion

**(1) The future challenges of regional data privacy will be striking the balance between protection and utilization of personal data within the organization such as ASEAN, APAA.**

**(2) As technology advances, the collection and utilization of regional data become more accessible, necessitating proper management. Transparency and regulatory enforcement, technological approaches such as anonymization and pseudonymization of personal data, and clarifying the purposes of use are crucial.**

**(3) Sufficient understanding and compliance with regulations are needed. Violation of regional data privacy regulation will lead to payment of huge penalties. Compliance will huge benefit such as regional close relationship and raising GDP, while protecting our privacy !**

# Thank you for your attention!

**Kozo Takeuchi**

**Japanese Patent Attorney**

**APAA President Elect**

kozo@takeip.jp