ASOCIO's Policy Guidance on Data Privacy:

Preserving Privacy while Enhancing Access to Personal Data with Greater Trust in Asian-Oceanian Region

Document Purpose

This document has been prepared to provide guidance on issues and policy to ASOCIO members and other interested stakeholders on current and proposed approaches to preserve privacy while enabling and enhancing trusted access to personal data. It can be used as a general background for the development of policy by ASOCIO members and for discussions with government officials and policy influencers.

DISCLAIMER

ASOCIO's Policy Guidance contains general information only and is not a substitute for obtaining advice specific to country legal systems and individual situations. ASOCIO does not accept liability for any action taken based on the information presented in this guidance or for any loss suffered as a result of reliance on this guidance.

Abstract

Our privacy is encapsulated in the data that identifies us privately, professionally or socially, and can easily be exploited to harm us. We need to protect it. Equally, we have always needed to share much of this data with others (eg, health/medical, banking/finance, tax/social security) in order to establish trust and interact efficiently and effectively, especially in the digital world. We expect those with whom we share such data to respect the need to protect it, and thereby protect our privacy.

The privacy pact described above is a balancing act between protecting and sharing. Businesses, governments and individuals must all respect the pact, and regulations must reflect it and the privacy-trust balance it embodies.

These issues are amplified where data is transferred across borders, and this ASOCIO paper offers policy guidance in that respect, especially to enable and maintain cooperation and collaboration within the region, and beyond.

ASOCIO's approach reflects 'good' practices adopted in Europe (through the GDPR), Japan (APPI) and within APEC (CBPR), based on three principles:

1. Risk-based, where protection requirements are relative to scale, data type/sensitivity, and transfer frequency;
2. Accountability, where there is mutual recognition of, and interoperability with, existing/planned data governance certification to avoid duplication, delay or fragmentation (as embodied in the GDPR and CBPR); and
3. Inclusive, where frequent, open consultations with data protection specialists, businesses, lawmakers and consumer groups occur transparently. These raise consumer trust, reduce compliance costs and minimise legal complexity.

ASOCIO urges all privacy and data protection stakeholders to examine and adopt this principle-based approach, drawing on good models and frameworks already developed and, in some cases, operating. Adopting the approach will promote freer, safeguarded data flows that enable regional economic growth and closer cooperation across the region.

About ASOCIO

The Asian-Oceanian Computing Industry Organization (ASOCIO) is a grouping of IT industry associations representing economies in the Asia Pacific region. ASOCIO was established in 1984 with the objective to promote, encourage and foster relationships and trade among its members, and to develop the computing industry in the region.

Presently, ASOCIO represents 24 members from Australia, Bangladesh, Bhutan, Brunei, Cambodia, Hong Kong, India, Indonesia, Japan, Korea, Laos, Macau, Malaysia, Mongolia, Myanmar, Nepal, New Zealand, Pakistan, Philippines, Singapore, Sri Lanka, Taiwan, Thailand, and Vietnam. Today, ASOCIO's members comprise more than 10,000 ICT companies and represent approximately US$350 billion of ICT revenue in the region.

ASOCIO has established a Policy Task Force (ASOCIO PTF) to promote a common understanding of “digital” related issues across the Region. The objective of the ASOCIO-PTF is to collaboratively research, develop, articulate and coordinate an ICT business voice on key issues affecting the sector to policymakers in APEC, ASEAN and South Asia economies. This paper is the first in a series developed and published by ASOCIO in pursuit of that objective.

Our Audience (Who should read this Guidance)

This Guidance will be circulated widely to policymakers, consumers, business partners, and all ASOCIO member associations and companies, to raise awareness of privacy issues and ASOCIO’s acknowledgment of the importance of data protection.

Data Privacy, Access and Trust: The Issues

Our personal data – the information that identifies us privately, professionally or socially, the related social and commercial activities we undertake, and even our communicated private thoughts – can easily be exploited to harm us. Equally, it is necessary for us to share much of this data to do everyday tasks and engage with other people in today’s society; we do this to identify ourselves, establish trust and engage in the modern networked digital world.

The need to protect our personal data has been long established. Indeed, in the European Union, data protection is defined as a fundamental right. As other countries and regions follow suit, a key challenge is to enable data protection in a balanced way that supports the access and sharing we must undertake to promote trust, and to engage socially and commercially.

ASOCIO’s Approach

ASOCIO’s first collaborative effort of the Task Force aims to redress the global fragmentation of privacy protection policies including domestic regulations and cross border transfer rules, specifically focused on the Asian-Oceanian region.

Through this effort, ASOCIO seeks greater consistency and understanding of privacy protection rules, generally, in order to enhance “trust” in the digital economy within the ICT industry, and specifically with business partners, consumers and society across the Asian-Oceanian region for social and economic exchange. More consistency and a better understanding of these rules will enhance access to, and sharing of, personal data that is the fundamental resource in the next generation economy and society (see, for example, Japan’s “Society 5.0” vision). ASOCIO members acknowledge this as central to their business across the region and urge policymakers to understand and adopt consistent rules that preserve privacy while enhancing access to personal data with greater trust.

ASOCIO calls for all governments across the Asian-Oceanian region – individually, and collectively through regional arrangements such as ASEAN, APEC, as well as in ongoing trade discussions – to develop and implement effective and consistent governance rules that enhance access to personal data with greater trust.

Governance of personal data that is effective and well understood through a generally common approach is vital to the digital economy of the ASOCIO region; it is equally vital for the region to grow effectively in global economic and social significance. We need to establish and promote our own common understanding of data governance specifically for personal data and continually improve the region-wide “trust" in the ICT/digital sectors using that personal data, as represented by ASOCIO.

To achieve this, ASOCIO recommends an approach based on three key principles to privacy protection in this guidance. In summary, ASOCIO recommends privacy protection that is:

1. Risk-based
2. Accountability based; and
3. Inclusive

Background

Since 2010, 30 years after the original 1980 OECD Privacy Guidelines, a new generation of personal data protection legislation has emerged or evolved in many countries. Currently, the Guidelines are undergoing a second review process within the OECD, including discussions on cross border data flows and accountability-based data governance.

Global fragmentation in privacy protection policies is a common concern for all stakeholders who are linked in the digital economy. This undermines opportunities for global/regional trade, as well as social and economic cooperation and collaboration.

ASOCIO’s ICT-related membership represents the "Digital Enabler Businesses" in the Asia-Oceania region. In this paper, ASOCIO seeks:

- initially to highlight the importance of raising awareness of national and regional policy stakeholders in privacy protection and enhancing trust;
- subsequently, to promote greater understanding and develop a common view; and
- finally promote unified policy and regulatory recommendations with our partners across the region.

It is critical to highlight the central importance of "trust" in the digital transformation of economies -- internally, and externally for trade, cooperation and collaboration within regions and globally.

Policymaking discussions must recognise the role and interdependence of data protection and privacy balanced with enabling enhanced access to personal data in promoting “trust” in the digitally-transformed economy.

ASOCIO advocates the importance of the “Digital Enabler Business” sector it represents working together internally across national borders to promote "trust" in the sector. Strong, consistent processes enabling effective governance of privacy and secure handling of personal data should be highlighted and must be understood by all members in ASOCIO.

ASOCIO will promote its position in privacy protection clearly and strongly to business partners, consumers, and policymakers across the Asian-Oceanian region.

ASOCIO and its members will advocate to, and work with APEC, OECD and other organisations focusing on privacy protection to encourage and achieve better coordination in cross border collaboration.

Thus, to ensure an effective response to these expectations, ASOCIO is sharing this guidance openly and widely with all ASOCIO members, partners, and policymakers to promote adoption of the principles and approach proposed.

ASOCIO Proposes:

ASOCIO proposes a simple approach based on three key privacy principles to enhance trust.

1. Risk-based privacy protection

It is not possible in practice to have “perfect” protection of personal data; unpredictability and uncertainty always exist in data handling; hence, without a risk-based approach, persistently seeking "always perfect" data protection results in excessive and unbalanced resource allocation to data governance without counterweight benefits to business, consumers, economies and society in general.

An effective risk-based approach must consider issues of scale: for example, SME processors of personal data, who handle small data holdings may have an optimized governance strategy for those needs, which will be significantly different to large processors of personal data. Policymakers should acknowledge ‘reasonable effort’ in the assessment of risks in the context of data holding type/sensitivity, scale and frequency to ensure optimized resources in business are based on these scales, proportionate to the real risk.

These risk assessments should acknowledge and reflect the many current positive experiences in existing secure cross border data transfer arrangements as strong evidence of lower overall risk in the longer term.

To enable efficient and effective risk assessment of the cross border transfer of personal data, ASOCIO recommends transparency of data handling processes on both sides of the

data transfer transaction. A good example of this risk-based approach can be found in the European Union's General Data Protection Regulation (GDPR), where three conditions to enable the cross-border transfer of personal data exist. These are:

- where there is data subject consent; or
- where the transfer is to a mutually recognized region/country with adequate data protection; or
- where the transfer occurs under designated model contract clauses.

Japan's Act on the Protection of Personal Information (APPI) has three similar conditions on cross border transfer of personal data, and also highlights mutual recognition of globally accepted certification mechanisms such as the APEC CBPR (Cross Border Privacy Rules System) as one of those conditions that enhances and facilitates cross-border collaboration for improved sharing and value creation by data. Nine APEC economies including Japan, Singapore, Korea, Australia, Chinese Taipei and the Philippines in ASOCIO region will have participated in CBPR by the end of 2019.

The "risk" does not just relate to data subjects; ASOCIO member companies can (and should) also mitigate their own risk by considering and implementing fair and appropriate protection of personal data. Thus, the benefits of establishing and maintaining "good but not perfect" risk management of data privacy as a key element of corporate-wide data governance are balanced with the costs.

Consistent with a risk-based approach to privacy protection, ASOCIO equally recommends policymakers in the region establish or ensure clear and transparent rules for risk-based cross-border transfer rules that are consistent with those already in place (EU's GDPR; Japan's APPI) or recommended as "good practice" within the region (APEC's CBPR).

2. Accountability-based privacy protection

"Accountability" is an important bridging concept to address the fragmentation in the global regime of privacy rules. The EU's GDPR also incorporates this concept.

Looking at the ASOCIO region, the APEC CBPR system is also based on "accountability", and the "Accountability Agent" in each economy coordinates its certification process. Here, the data accountability-based approach enables an alternative to governmental direct regulation: instead of defining the rules and legislation, controllers and processors define their own "accountability" in a clear, written form to share among employees, business partners, consumers and society as a whole.

Singapore, Japan, Republic of Korea, Australia and Chinese Taipei have already joined in the CBPR scheme, along with non-ASOCIO (but APEC) economies USA, Mexico, and Canada. The APEC Data Protection Subgroup (DPS) is planning outreach of the CBPR system to non-APEC economies such as economies in South Asia. ASOCIO members, together with their members and governments should engage with this DPS outreach program.

Interoperability with expected certification mechanisms in EU/GDPR is also a priority of CBPR promotion. ASOCIO expects that because of the consistent accountability principles, recognising and adopting common items in accountability checklists should further reduce

fragmentation in privacy protection frameworks as the APEC model is adopted and other national frameworks emerge in the region.

To encourage this further within ASOCIO and its members and partners, opportunities to work collaboratively on consistently accountability approached must be created and practiced. These should include evidence-based research, educational materials, seminars, peer reviews and virtual forums; together, these can effectively raise the accountability ethos and mind-set by sharing experiences and knowledge among ASOCIO businesses including SMEs.

3. Inclusive privacy protection for trust

Government access to personal data should be limited to minimum requirements to serve the needs of their citizens; public sector governance of personal data must itself be undertaken using democratic principles and market-based processes.

Privacy protection depends upon a multistakeholder approach. ASOCIO will work with associations in each economy, consumers, and specifically SMEs in this region. Specifically, APEC's Digital Economy Steering Group and its Data Protection Subgroup are at the centre of the CBPR program.

An inclusive approach, both within ASOCIO and in collaboration with other international public policy advisory groups is required, and frequent, open consultations with specialists in data protection will be important.

Equally, raising consumer trust is essential: on the one hand, consumers express concern about the sharing and handling of their personal data; on the other, consumers willingly and openly participate in the digital world for a variety of social and commercial reasons. Trust, implicit or explicit, underpins this and it is a mutual requirement. Hence, government and business initiatives to facilitate and enhance trust must be persistently undertaken. ASOCIO and ASOCIO members can initiate these. The benefits of these are well-known: creation of strong, branding effects, reducing/optimising costs of compliance and legal requirements.

Enhanced consumer trust will, in turn, facilitate inclusive free data flows in Asian-Oceanian region. These promote the more open, fair and market-based digital economy that enables the growing, broader national digital ecosystems essential for national and regional economic growth. ASOCIO will support free data flows discussion such as in APEC, ASEAN, and FOIP (the Free and Open Indo-Pacific Strategy).

Conclusion

Fair and good (as opposed to "perfect") knowledge and appropriate governance in privacy protection is essential to develop new business in the digital economy. Thus, all ASOCIO stakeholders, their governments and policymakers are urged to consider and adopt *risk-based*, *accountability-based* and *inclusive* principles in their approach to data protection to increase trust and enhance access.

Good models and frameworks exist; some are in use; collaborative development of these models/frameworks in the context of the region provides an importantopportunity to create

an Asian-Oceanian free data-flow trade area, providing significant national and regional economic growth, and opportunities for closer cooperation across all levels of society.

All ASOCIO members and interested stakeholders are invited and encouraged to join the conversations that are necessary for these outcomes to be realised – through ASOCIO itself and/or by participation in stakeholder/observer groups to organisations such as the APEC Digital Economy Steering Group.

Acknowledgement

This policy guidance has been prepared by ASOCIO's Policy Task Force, whose time, effort and contribution is gratefully acknowledged. Members of the 2019 Policy Task Force:
Mr Seiichi Ito (JISA — Chair of PTF), Mr David Wong Nan Fay (Chair — ASOCIO), Mr Woon Tai Hai (Secretary-General — ASOCIO), Mr Bunrak Saragganda (ATCI), Mr Abdullah H Kafi (BCS), Dr John Choi (FKII), Mr Rajesh Nambiar (NASSCOM), Dr Junko Kawauchi (JISA), Mr See Kiat Yeo (SGTech), Prof Makoto Yokozawa (JISA), Ms Lee Sook Han (SGTech), Prof Jarernsi Mitrpanont (ATCI), and Mr Tim Conway (Australia - Consultant)