



**Asia-Pacific
Economic Cooperation**

**TRADE POLICY DIALOGUE ON FOSTERING AN ENABLING
POLICY AND REGULATORY ENVIRONMENT IN APEC FOR DATA-
UTILIZING BUSINESSES**

23 August 2019, Puerto Varas, Chile

FINAL REPORT

Appendix

~ IX. PRESENTATION MATERIALS ~

APEC Committee on Trade and Investment

December 2019

TABLE OF CONTENTS

IX. PRESENTATION MATERIALS	3
A. Mr Andre Wirjo, Analyst, APEC PSU	3
B. Dr Peter Hendy, Aegis Consulting Group	13
C. Mr Nigel Cory, Information Technology and Innovation Foundation	19
D. Dr Makoto (Mac) Yokozawa, Kyoto University, Japan.....	29
E. Dr Peter Lovelock, Director, TRPC	38
F. Ms Karina Kudakaeva, Researcher, Institute for International Economics and Finance, Russian Foreign Trade Academy	46
G. Mr Alex Mauricio Pessó Stoulman, Legal, Corporate Affairs and Philanthropies Director, Microsoft Chile	53
H. Mr Hiromu Yamada, JIPDEC	58

Appendix

IX. PRESENTATION MATERIALS

Presentation materials for all speakers follow below.

A. Mr Andre Wirjo, Analyst, APEC PSU



Outline

- 1) Overview
- 2) Study objective and approach
- 3) Role of data
- 4) Challenges across economies
- 5) Way forward



Copyright © 2019 APEC Secretariat

Overview

- The [use of data and analytics are widespread](#) across APEC businesses.
- [Their importance will only increase](#) in the future thanks to more connectivity, big data, internet of things (IoT) and artificial intelligence (AI).
- There is increasing evidence on the [contribution of data to economic growth, productivity and employment](#).
- Recent initiatives on digital economy in APEC include [APEC Framework on Cross-border E-commerce Facilitation](#) and [APEC Internet and Digital Economy Roadmap \(AIDER\)](#).

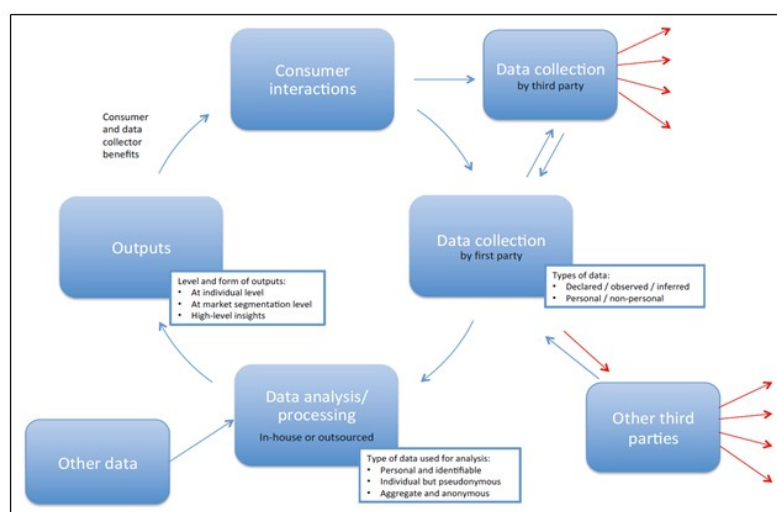


Copyright © 2019 APEC Secretariat

-
- Percentage of participating firms*
- by economy*
- | Economy | Percentage |
|---------|------------|
| JPN | 22% |
| SGP | 11% |
| VN | 14% |
| USA | 8% |
| CT | 8% |
| AUS | 8% |
| CDA | 6% |
| MAS | 6% |
| PHL | 8% |
| MEX | 3% |
| CHL | 3% |
| INA | 3% |
- by firm size*
- | Firm Size | Percentage |
|-----------|------------|
| Large | 53% |
| Medium | 33% |
| Small | 14% |

- 

Role of data



Role of data in selected sectors



Transport and logistics

- Use personal data collected during flight booking to develop attractive loyalty schemes.
- Share data with partner firms for more seamless travel experience.
- Use performance data of assets to assess efficiency of asset deployment.



Manufacturing

- Use performance data of sold and leased assets (collected remotely) to schedule maintenance, prepare immediate replacements and reduce downtime.
- Track data on inventories to facilitate reordering process.



Healthcare

- Use data for collaborative research activities.
- Share data between institutions to facilitate diagnosis (sometimes remotely).



Asia-Pacific
Economic Cooperation

Copyright © 2019 APEC Secretariat

Role of data in selected sectors



Payment and electronic invoicing (EI) services

- Summarize traditional and structured data in form of standard daily transactions report to merchants.
- Use credit incidents and debt data to predict likely customer behavior.
- Use data captured in EIs to facilitate transparency and compliance.



Other data analytics services

- Use hybrid techniques on data to recognize pattern, detect anomaly and combat fraud.
- Screen employees, contractors and tenants against different databases (e.g. criminal records, motor vehicle records)



Asia-Pacific
Economic Cooperation

Copyright © 2019 APEC Secretariat

Role of data in selected sectors

Manufacturing

Pre-production	Production	Post-production
<ul style="list-style-type: none">• Design and conceptualization• R&D• Prototyping• Testing• Market research	<ul style="list-style-type: none">• Coordination between production facilities• Communications with suppliers• Production planning• Monitoring production on floors• Scheduling maintenance and repair services	<ul style="list-style-type: none">• Quality assurance/ quality control• Communication with logistics providers• Remote monitoring of sold products

Source: Authors



Asia-Pacific
Economic Cooperation

Copyright © 2019 APEC Secretariat

Role of data

Findings across sectors

- Firms recognize the value of data on their businesses viability, and consider that adequate protection of personal data as necessary and part of the [social contract to operate](#).
- For this reason, they have undertaken a [range of measures](#), including:
 - Ensure consistency of their policies, procedures and practices with international [QA instruments](#).
 - Undertake regular and systematic review of various [laws and regulations](#) and ensure compliance.
 - Apply sophisticated and [comprehensive data governance frameworks](#) in different areas (e.g. hardware, cyber protection teams, encryption).



Asia-Pacific
Economic Cooperation

Copyright © 2019 APEC Secretariat

Challenges across economies

Calls for more data privacy, protection and security

- Importance of data has naturally brought concerns on how firms use and protect data.
- Fears are not unfounded.
- In response to the calls for better data protection and security and other public policy objectives (e.g. rapid access, employment, investment), data-related regulations enacted include:
 - Local data storage, processing and/or transfer.
 - Disclosure of IP (incl. source code), building back-doors and use of mandatory encryption standards.



Asia-Pacific
Economic Cooperation

Copyright © 2019 APEC Secretariat

Challenges across economies

But are some of these regulations the way forward with regards to the following?



Data protection and security

- Function of several elements incl. technical, financial and personnel.
- May not be necessarily strengthened when data is localized.



Employment and investment creation

- Employment may not be as rosy as expected.
- Demand-driven investment continues.



Innovation and productivity

- May inadvertently be affected negatively.
- Have to be complemented with other regulations (e.g. strong IPR protection).



Domestic security

- First-best options focusing on access available.



Asia-Pacific
Economic Cooperation

Copyright © 2019 APEC Secretariat

Challenges across economies

Alternative/middle-ground approaches

- Encouraging and recognizing the [adoption of industry standards](#).
- [Enhancing domestic regulations](#) by reviewing against privacy guidelines/framework; and complementing lighter touch regulations with effective enforcement.
- [Enhancing cross-border data flows](#) through tangible measures such as the recognition of privacy certifications/seals (e.g. CBPR), the inclusion of cross-border mechanisms for data transfers in RTAs/FTAs, the negotiation of multilateral rules for cross-border data transfers, etc.
- [Improving domestic security](#) through mechanisms such as reform to mutual legal assistance treaties (MLAT), bilateral/multilateral data sharing via MoUs and unilateral approaches focusing on mandating access as opposed to location.



Asia-Pacific
Economic Cooperation

Copyright © 2019 APEC Secretariat

Alternative/middle-ground approaches

What are they?

- Those with relatively minimal/less impact of data-utilization by firms and concurrently, fulfill legitimate public policy objectives.
- Bridge between what governments/policymakers want and what businesses need.
- Pragmatic approaches to data-related regulations.
- Complementary.
- Steps in the right direction and can be improved further.



Asia-Pacific
Economic Cooperation

Copyright © 2019 APEC Secretariat

Alternative/middle-ground approaches

Industry standards

- Provide baseline requirements in areas such as privacy and security protocols, policies and rules (e.g., ISO27001 and BS10012).
- Usually consistent (in intent) with data protection legislation in economies (governing data flow and use in B2B and B2C).
- Adherence has been used as a way to build trust by businesses.
- If insufficient, possible to work with industry to fine tune standards to address policymakers' concerns or come up with something complementary?



Copyright © 2019 APEC Secretariat

Alternative/middle-ground approaches

Domestic regulations

- Major role of domestic regulations on enforcement.
- But important to ensure regulations do not go beyond the original remit/intent.
- Review existing and potential regulations against privacy guidelines/framework (e.g., APEC Privacy Framework, OECD Guidelines) – formulated in the spirit of cooperation.
- Complement lighter touch regulations with effective enforcement (e.g., civil and administrative incl. fines, and criminal sanctions).



Copyright © 2019 APEC Secretariat

Alternative/middle-ground approaches

Cross-border data flows

- Focus on effective regulations (as opposed to strict bans).
- Recognition of privacy certifications/seals and related mechanisms (e.g. CBPR).
- Carve in frameworks for cross-border data transfers in RTAs/FTAs (e.g. CBPR in USMCA, CPTPP).
- Explore mechanisms for facilitating adequacy status to partners (e.g. GDPR & Japan, US-EU Privacy Shield).
- Continue with discussions on cross-border data flows at the multilateral level.



Copyright © 2019 APEC Secretariat

Alternative/middle-ground approaches

Domestic security

- Explore and enhance other mechanisms (beside data localization) to improve security.
- Reform mutual legal assistance treaties (MLAT) (i.e., agreements to ease exchange of information) (e.g., Annex to Budapest Convention on Cybercrime).
- Promote bilateral and multilateral data sharing (e.g., Automatic Exchange of Financial Account Information between INA and SG, draft legislation by US DOJ).
- Mandate access to specific data regardless of location (e.g., Dodd-Frank Act, accounting data in Denmark).



Copyright © 2019 APEC Secretariat

Alternative/middle-ground approaches

Recognizing limitations while improving and complementing approaches




- [GDPR adequacy status] Difficult to obtain.
- [GDPR standard contractual clauses] Currently under debate for not adequately protecting data of EU individuals against government surveillance.
- [APEC CBPR] Awareness among firms; awareness \neq participation; number of participating economies; interoperability with other systems.
- [GATS] Coverage of new digital services by existing commitments; openness of some sectors still subject to exceptions within the agreement.



Copyright © 2019 APEC Secretariat

Way forward

Recommendations for APEC

-  **Facilitating information and experience sharing/exchange** on the alternative/middle-ground approaches to data-related regulations.
-  **Organizing dialogue sessions** to identify ideas and ways to overcome bottlenecks that have led to standstill or little progress in some of these approaches.
-  **Developing capacity-building activities** to assist member economies in enhancing and improving their existing data-related and complementary regulations, including those pertaining to IPR protection as well as transparency of regulations.



Copyright © 2019 APEC Secretariat

Find out more

APEC Online and Social Media



apec.org



[@APECnews](https://www.facebook.com/APECnews)



[@APEC](https://twitter.com/APEC)



[@apec](https://www.instagram.com/apec)



[APEC – Asia-Pacific Economic Cooperation](#)



Asia-Pacific
Economic Cooperation

Copyright © 2019 APEC Secretariat

B. Dr Peter Hendy, Aegis Consulting Group



CTI Trade Policy Dialogue on “Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses” – Chile, 23 August 2019

Presentation on key findings from consultations with firms in the transport and logistics, e-commerce, consumer services and manufacturing sectors

Trade Policy Dialogue on Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses

Methodology

- ▶ The views of individual companies have been gained via their written responses to a questionnaire and/or interviews.
- ▶ We asked 64 companies to participate in the research. These companies were nominated by APEC economies or Aegis Consulting Group from its client base and network.
- ▶ Of those asked, 33 companies (53 percent) agreed to do so.
- ▶ Most companies asked to remain anonymous and for their supplied information to be treated confidentially in the report.
- ▶ Many responses lacked detail, despite specific questions designed to obtain it.
- ▶ Additional consultations were held with trade groups in Singapore, Chinese Taipei and Japan via workshops and roundtables. Industry sectors represented at these forums included those from which individual companies were drawn as well as financial and legal services.

Final 050819

2

Profile of firms - 1

- ▶ The participating firms were spread across 8 APEC economies – Australia, Chinese Taipei, Indonesia, Japan, Philippines, Malaysia, Singapore and Vietnam.
- ▶ **The 33 firms operate in the following industry sectors:**
 - ❖ 9 firms in aviation, logistics (postal and infrastructure management) and transport (shipping and railways).
 - ❖ 14 firms in e-commerce (software services at enterprise level, data analytics for business customers, internet support including storage, information security, e-commerce including online retailing and business information systems)
 - ❖ 4 firms in consumer services (energy, healthcare and education publishing).
 - ❖ 6 firms in manufacturing (automotive, industrial robots, semiconductors, consumer electronics and goods, avionics, entertainment systems, mobile and camera products, elevators, railways, power generation systems, magnetic materials, wires and cables, excavators, wheel loaders, trucks, cranes, and demolition equipment).
- ▶ All but 3 firms are involved in cross border trade.

Final 050819

3

Trade Policy Dialogue on Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses

Profile of firms - 2

- ▶ Good diversity of firms providing B2B and/or B2C services/products.
- ▶ Reasonable diversity of enterprise size. Largest company has 300,000 employees and the smallest has 6 people. Research includes established conglomerates and start ups.
- ▶ **Most firms reported using data for:**
 - ❖ Customer management - provide services and maximise consumer choice and convenience.
 - ❖ Operational efficiency - improve supply chain management and efficiency to reduce pre and post production costs.
 - ❖ Service innovation - better align supply side distribution processes with demand in B2B and/or B2C markets.
- ▶ **Some firms reported using data to:**
 - ❖ Harmonise back of office functionality.
 - ❖ Promote service and product value and appeal to support competitiveness.
- ▶ All firms store data in one or more ways – (1) cloud services; (2) local servers; and (3) remote servers.

Final 050819

4

Firms are strongly motivated to apply best practice data management

- ▶ **Firms understand that protecting the privacy data in their possession and deploying comprehensive information security for data flows and use is essential to:**
 - ❖ Maintain the reputation of their brands and business models in the marketplace.
 - ❖ Build and retain community trust in the management of data they transfer to firms.
- ▶ To meet market expectations most firms apply policies that are consistent with international information security standards - ISO27001 and BS10012.
- ▶ These standards assist firms comply with privacy and personal data protection legislation in individual APEC economies governing data flows and use B2B and B2C activities.
- ▶ These standards also give firms a solid basis to begin their compliance with the European Union's General Data Protection Regulation (GDPR).
- ▶ Many firms are subject to the GDPR because their customers include EU citizens and/or EU businesses whose customers include EU citizens.

Final 050819

5

Common data management practices by firms regardless of data storage

- ▶ **Managing data flows within secure, transparent and auditable frameworks including:**
 - ❖ Using the most secure and trusted hardware and location when choosing storage infrastructure.
 - ❖ Employing cyber protection teams to design and operate selected hardware and the flow of data.
 - ❖ Applying end-to-end encryption on all data flows across borders and over the Internet. Encryption has been previously identified by APEC PSU as a legitimate alternative to regulation.
- ▶ **Deploying a sophisticated and comprehensive data governance framework including:**
 - ❖ Classifying and restricting access to data according to its sensitivity and systematically reviewing regulations to ensure compliance.
 - ❖ Appointing CIOs and reporting compliance at Board level.
- ▶ **Investing in staff education a training to increase cyber security awareness and compliance with company and government data management rules.**

Final 050819

6

Common views amongst firms about the benefits of regulation

- ▶ **Almost all firms believe that regulation delivers strong benefits for them which outweighs any compliance costs. These benefits are that:**
 - ❖ Regulation can be relied on to support brand reputation - helps communities and consumers trust that the data flows, use and management are safe and secure.
 - ❖ Regulation provides important support for their 'social licence to operate'.
 - ❖ Regulation helps to equalise data management practices in international trade and enables firms doing the wrong thing to be 'called out'.
 - ❖ As data use increases regulation has an important role to play in maintaining an overriding market and community confidence in digitalisation and digital trade.
 - ❖ The increasing use of machine learning and artificial intelligence will require regulation to avoid malpractices.

Final 050819

7

Common views amongst firms about the costs of regulation - 1

- ▶ Regulatory compliance can create direct administrative costs. This includes the cost of legal reviews, hiring or engaging specialist cyber security staff and training staff.
- ▶ Opportunity costs of regulation vary but include restrictions on trading activities, decreased competitiveness and reduced investment in innovation.
- ▶ **Direct and opportunity costs are elevated by a range of issues including:**
 - ❖ Poor regulatory transparency which deters trading.
 - ❖ Localisation requirements for data storage require firms to duplicate infrastructure and data handling costs and market entry can be restricted when these costs are too high.
 - ❖ Demands by governments for data sharing. This can limit market entry when firm data management policies do not permit the transfer of customer's personal data to third parties.
 - ❖ Lack of intellectual property enforcement also reduces incentives for market entry and trading arrangements such as joint ventures.

Final 050819

8

Common views amongst firms about the costs of regulation - 2

- ▶ Different prioritisation given to data control can be problematic. For example compliance costs increase when firms are required to satisfy regulatory regimes with diverging assumptions about data being owned by the state, individual or corporation.
- ▶ There is inadequate regulatory alignment between economies because of varying approaches to the fundamental rights to privacy, domestic sovereignty and related rights to data and domestic security concerns in data flows.
- ▶ Most companies have a strong view that economies need to work harder to ensure that they pursue a more consistent and aligned approach to data regulation within and between economies and in bi-lateral free trade agreements and multi-lateral agreements.
- ▶ It was suggested that the Comprehensive and Progressive Agreement for Trans Pacific Partnership (CPTPP) Chapter 14 offers a good opportunity to achieve this alignment.
- ▶ Most companies were not aware of APEC's Privacy Framework, Cross Border Privacy Rules (CBPR) or the work APEC is doing to promote the interoperability between the CBPR and EU's GDPR.

Final 050819

9

Trade Policy Dialogue on Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses

Common firm preferences about regulation

- ▶ Regulatory frameworks should consider that companies have strong commercial reasons to apply best practice data management practices and regulation should serve to enhance, not duplicate the measures companies already take.
- ▶ APEC should increase private sector awareness of its Privacy Framework, Cross Border Privacy Rules (CBPR) and its work to ensure the interoperability between the CBPR and EU's GDPR.
- ▶ Regulatory frameworks should recognise that companies have global activities and customers and costs increase when regulation is unaligned and inconsistent. APEC economies should work towards increased regulatory alignment between them under the World Trade Organisation frameworks.
- ▶ APEC should examine in more detail the appropriate regulatory arrangements for artificial intelligence as this is an important means for MSMEs to participate in the global value chain in innovative ways.

Final 050819

10

Common trade group references about regulation

- ▶ Alignment of digital trade research being conducted by relevant APEC fora.
- ▶ Spectrum licensing by governments should be consistent with the general data regulation.
- ▶ Data regulation should not impede open source policies, particularly for government controlled information.
- ▶ Regulation should recognise that markets value social media and search engine companies based on what companies know about the purchasing and recreational preferences and connectivity of each customer. This means regulation should strike the appropriate balance between promoting the tradeable value of information and data privacy.
- ▶ Government investment in 5G infrastructure to support data flows needed for business sustainability and competitiveness.
- ▶ Government investment in the study of science technology engineering and maths (STEM) within their communities to overcome future skill shortages in digital capability.

Final 050819

11

Thank you. Questions?

Final 050819

12

C. Mr Nigel Cory, Information Technology and Innovation Foundation

**Fostering an Enabling Policy Environment for
Data-Utilizing Businesses: AI, payments,
encryption, and accounting/tax services**

Nigel Cory
Associate Director, Trade Policy, ITIF

August 23, 2019

@Nigelcory
ncory@itif.org

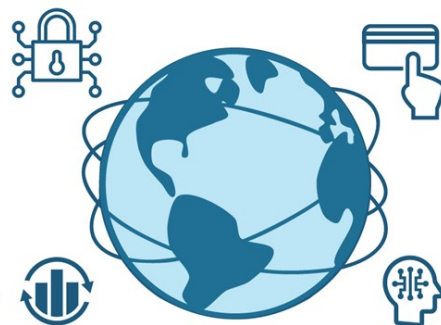
The Information Technology and Innovation Foundation (ITIF)

- Independent, nonpartisan research and education institute focusing on intersection of technological innovation and public policy, including:
 - Innovation and competitiveness
 - IT and data
 - Telecommunications
 - Trade and globalization
 - Life sciences, agricultural biotech, and energy
 - Formulates and promotes policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress
 - World's top think tank for science and technology policy, according to the University of Pennsylvania's authoritative *Global Go To Think Tank Index*
-

ITIF | INFORMATION TECHNOLOGY
& INNOVATION FOUNDATION 2

Overview

- Payment Services and Digital Trade
- Encryption Services and Digital Trade
- Electronic Invoices and Digital Trade
- Artificial Intelligence and Digital Trade
- Conclusion:
 - From the Firm and Policymaker's Viewpoints
 - For the Future of Digital Trade Policy



ITIF | INFORMATION TECHNOLOGY
& INNOVATION FOUNDATION 3

Payment Services and Digital Trade

- Tech and market changes: Incumbent payment services vs. fintech.



- Firm A: U.S.-based global multinational financial services firm.
- Payment services and digital trade are inseparable: but restricted.
 - ITC survey: 23 percent of 2,200 MSME respondents from more than 100 economies identified e-payment services as a major obstacle.

Payment Services, Data Use/Flow, & Barriers

- Data is central: payment networks clear and settle transaction information, not funds.
- Data restrictions on a sliding scale of impact
 - Mirroring of data => full and only local data storage => local data processing and routing.
 - Acts as market barrier & discriminates against foreign firms, especially SMEs.
- E.g. Indonesia, Russia, India, Viet Nam, and elsewhere.



Impact of Restrictions on Payment Services Data

- Limits use of globally distributed data analytics platforms
 - Cost/technical feasibility of pulling down global platform to local IT ecosystem.
- Impacts:
 - Less innovation: Firm A uses diverse data sets to drive innovation.
 - Security risks: Firm A needs global data to fight money laundering & fraud.
 - Lower firm competitiveness and economic productivity:
 - Prevents access to best and lowest cost provider.

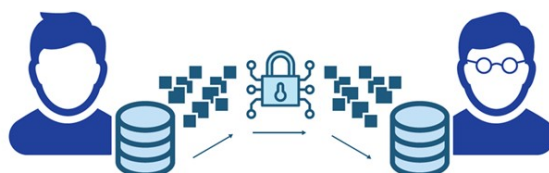


ITIF | INFORMATION TECHNOLOGY
& INNOVATION FOUNDATION 6

Digital Trade and Encryption: An Overview



- Encryption is ubiquitous to digital trade:
 - It protects security/confidentiality of data and services.
- Firm: U.S.-based Virtru provides client-side encryption services.
- Protection, flow, and use of data is critical to Virtru's business model.



ITIF | INFORMATION TECHNOLOGY
& INNOVATION FOUNDATION 7

Digital Trade and Encryption: Policy

- Constructive policy: Economies require firms use “technical measures” to protect sensitive data to mitigate data protection concerns.
 - E.g. European Union’s GDPR, health & payment data in United States.
- Policy that undermines encryption:
 - Local key & data storage, source code disclosure, backdoors/tech assistance, & discriminatory licensing.
 - Undermine core functionality and integrity/security of encryption services.



ITIF | INFORMATION TECHNOLOGY
& INNOVATION FOUNDATION 8

Electronic Invoicing (EI) and Digital Trade: Overview

- Many benefits to EIs:
 - Support traditional/digital trade. E.g. more efficient ‘factoring.’
 - Efforts to combat fraudulent activities and improve tax and other business services.
- Firm: Chile-based GoSocket
 - Uses cloud-based services to operate across Latin America.
 - Over 20,000 firms processing 5 million EIs daily.



ITIF | INFORMATION TECHNOLOGY
& INNOVATION FOUNDATION 9

Electronic Invoicing: Legal/Regulatory Issues






- EIs involve data, data flows, and cybersecurity issues.
 - E.g. e-signatures and certificates to certify parties and protect integrity/security of EIs.
- Economy-specific technical requirements undermine cloud-based EI services.
 - Brazil: Use of local tech standard and local IT services for e-signatures.
 - Mexico: Until recently, required local storage of digital certificate, which equals de facto data localization.

Electronic Invoicing: Impact and Solution

- Mexico made the smart correction:
 - Allowed providers to use cloud-based hardware security modules, which use best-in-class, audited/certified cybersecurity measures.
- GoSocket example shows:
 - Behind-the-border technical measures can act as barrier to cross-border data flows, service provisions, and use of best-in-class security tools.
 - Need for holistic assessment and cybersecurity expertise in policymaking.

AI and Digital Trade: The Firms

- Mindbridge Ai is based in Ottawa, Canada. 
 - Uses AI/ML to investigate/audit past activity, detect active inadmissible behavior (e.g., fraud), and prevent potential transgressions.
- Pondera Lab is based in Mexico City, Mexico. 
 - Uses AI/ML to help firms and government agencies use AI to better organize, analyze, and visualize data to help make better business decisions.
- Certn is based in Victoria and Toronto, Canada. 
 - Uses AI/ML to help clients analyze prospective customers, employees, and renters.

Use of Data and Key Data-Related Policy

- As Certn put it: “business is data.” Same for all.
 - But for each firm, the source and use of data is different.
 - Collected or provided or mixed data sets; structured vs. unstructured; hosted on home cloud services or access provided to client’s data provider.
- Two sets of rules that affect use of AI for digital trade:
 - the rules on data; and
 - source code protection.



AI and Data Privacy/Protection

- Key point: Privacy regulations are central
 - All firms carefully consider data-related laws before entering a market.
 - Mindbridge Ai = built to “high watermark” of EU GDPR, in part, due to threat of major fines.
 - Certn = made up-front investment to help it be GDPR compliant. Also has to abide by province-level data localization in Canada.
- Firms (like Mindbridge Ai) operate from cloud services in key markets (Canada, US, and EU).

AI and Digital Trade:

- Privacy/data protection is competitive advantage.
- Formal laws only one piece of the puzzle:
 - Clients use contractual law to ensure additional legal protections:
 - E.g. where to store data and how to manage access to the data.
 - Firm itself demands additional steps above and beyond the law:
 - E.g. Additional technical and administrative controls.
 - E.g. Third-party auditing/certification services.

Protecting AI

- Source code of AI/ML is susceptible to exposure and theft.
- Multiple methods:
 - Source code protections (domestic laws, trade provisions (USMCA));
 - The use of strict contractual arrangements;
 - Strict control over AI development process; and
 - The use of technical and administrative controls to manage access and use.
- Many firms: refuse to enter and upload AI systems to cloud service providers in certain markets due to risks.

Conclusion: From the Firm's Perspective

- The optimal scale of a digital firm is global.
 - E.g. AI systems were designed for the cloud.
- Importance of economies of scale to digital businesses.
 - Core vs. non-core markets: Firms weigh up cost and complexity involved in tailoring (often global) IT systems for local conditions.
 - Sum of multiple minor regulatory differences/changes can add up and equal major barrier to digital trade.
- Unnecessary/overly restrictive artificial barriers prevent this.
 - Impact can be direct and indirect (customer risk aversion).

Conclusions: For Policymakers

- Policymakers challenge:
 - Grasping the challenges of today's data/AI-driven economy.
 - Understanding technology and intersection with policy issues.
 - E.g. Data localization ≠ data security. Data protection can flow with data.
 - Identify policy best-practices and the need to balance competing goals, such as consumer privacy, productivity, and innovation.
 - E.g. APEC's CBPR ensures data protection flows with the data, wherever it is stored.
 - E.g. Policies that encourage firms to use encryption and cloud-based cybersecurity measures.
-

Overall Conclusions for Digital Trade Policy

- The critical role of data and digital technologies and services.
 - Future of trade policy:
 - Central role of data means future trade policy will likely focus on these points of friction and/or bridges for interoperability.
 - Potential for long-term divergence: Interoperability vs. fragmentation.
 - Which norm prevails will play a part in determining the impact of AI and other data-driven technologies in driving economic productivity and innovation.
-

Thank You!

Nigel Cory | ncory@itif.org | @niglcory

ITIF | INFORMATION TECHNOLOGY
& INNOVATION FOUNDATION

@ITIFdc

D. Dr Makoto (Mac) Yokozawa, Kyoto University, Japan



**CTI Trade Policy Dialogue on
“Fostering an Enabling Policy and Regulatory Environment
in APEC for Data-Utilizing Businesses”**

【Date and Venue】 August 23, 2019 at Tronador, Enjoy Hotel in Puerto Varas, Chile

【Organizer】 Ministry of Economy, Trade and Industry, Japan, supported by Washington Core, L.L.C.

The Graduate School of Informatics, Kyoto University
“Business at OECD (BIAC)” Digital Economy Policy Co-Chair
Keidanren (Japan Business Federation) Global Strategy WG Chair
Nomura Research Institute, Ltd.

Prof. Makoto (Mac) Yokozawa

Copyright MOIS Research Unit, Kyoto Univ. 2019

Panel 1

Appropriate Policy and Regulatory Environment in Data Utilization

1

- **Some Considerations on Data with "Trust"**
 - We need to recognize the data in business
 - We need Proper "Classification" of Data

http://www.keidanren.or.jp/en/policy/2019/020_Examples.html

Policy Proposals Trade, Investment, EPA/FTA

B20 Tokyo Summit: Tangible Examples by Business
— Toward Society 5.0 for SDGs —



Attachment of "B20 Tokyo Summit Joint Recommendations"

3 GOOD HEALTH AND WELL-BEING



aspenmedical

ASPEN MEDICAL
(WWW.ASPENMEDICAL.COM)

AiGROUP

AUSTRALIA

Establishment of Primary Health Care Clinics across four African countries.

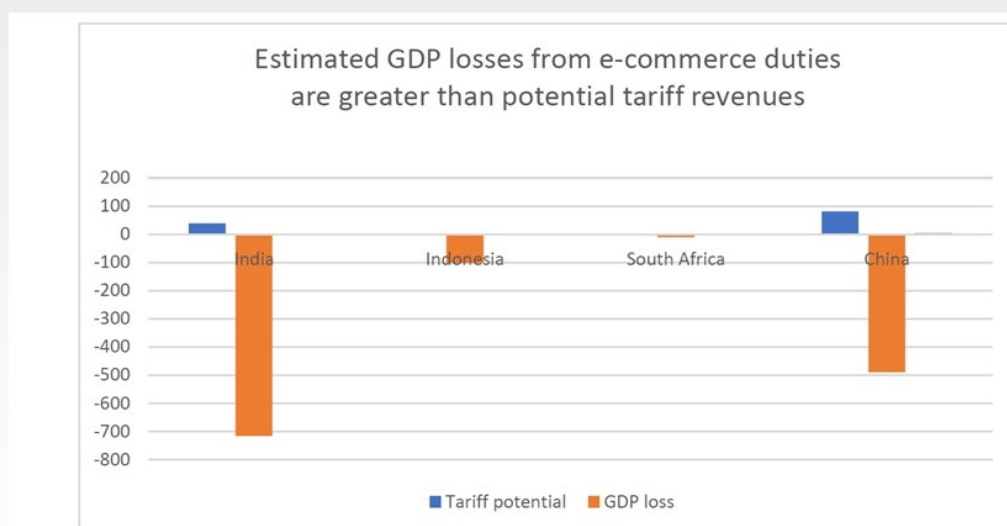


RELATED SDGS GOALS



stretched public services, 95% of the staff are African and all management roles are performed by females.

The Economic Losses from ending the Moratorium on Electronic Transmissions



Data from ECIPE study – assumes a scenario of reciprocal tariffs. Units in millions of US\$. Tariff estimates from UNCTAD 2017 report, *Rising Product Digitalisation and Losing Trade Competitiveness*.

Source: Hosuk-Lee Makiyama and Badri Narayanan (2019), "The Economic Losses from Ending the WTO Moratorium on Electronic Transmissions". https://ecipe.org/wp-content/uploads/2019/08/ECI_19_PolicyBrief_3_2019_LYo4.pdf

All Copyright Reserved 2014

Cross Border Data Driven Innovation ... Examples



Remote Monitoring/Maintenance of Construction Facilities



Sensor monitored logistics



Contents Delivery Networks



Remote Monitoring of EVs



Remote Monitoring/Management of Production Plants



Remote Monitoring of Large Ships



Remote Monitoring/Management of Agriculture



Human Behavior in Cyberspace



Remote Monitoring of Raw Foods



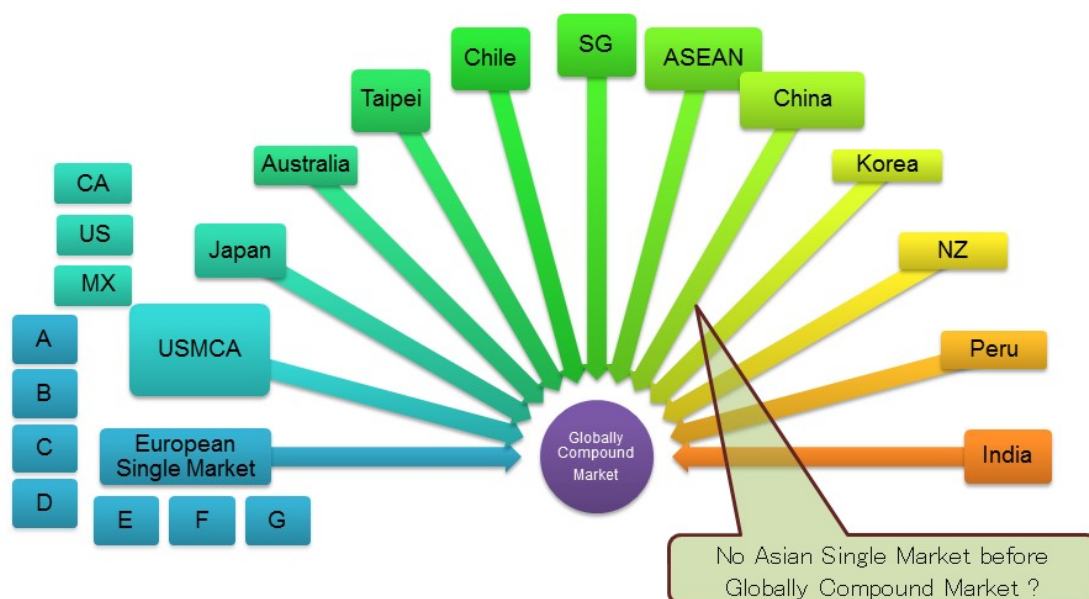
Wild Animal Monitoring

All Copyright Reserved 2014

3

Long-term Global Market Scenario

---Which is earlier, Globally Compound or Asian Single?



All Copyright Reserved 2014

4

Possible Updates in Scope

Taxonomic Classification of Data (example)



OECD “Data in the Digital Age” (promoting “enhanced access to data”)



Box 1. Disentangling different types of data

There is no one “right” way to classify data into different types. One approach that could be relevant to policy making distinguishes the parties involved in data flows and assigns a proximate assessment of the personal content of that data. The example below is for illustrative purposes, to show the variations that may exist across data types.

Type of data	Personal content
Business to Business (B2B)	0 1 2 3 4 5 6 7 8 9 10
GVC data	→
Engineering (M2M)	→→
IoT (M2M)	→→→
Financial / human resources	→→→→
Business to Consumer (B2C)	
Media	→→→→
Consumer	→→→→→
Services (e.g. health, financial)	→→→→→
Government to Citizen (G2C)	
Services (e.g. health, tax, identity, social-welfare protection)	→→→→→
IoT (e.g. metro, CCTV)	→→→→→
Citizen to Citizen (C2C)	
Social media	→→→→→
Communications (e.g. e-mail, messages, voice)	→→→→→

Notes: GVC = global value chain; M2M = machine-to-machine ; IoT = Internet of Things; CCTV = closed-circuit television. Scale of personal content from 1 to 10, where 1 is low personal content and 10 is high personal content.

Source: Based on OECD (forthcoming a), *Enhanced access to and sharing of data: Reconciling risks and benefits of data re-use across societies*.

7

ISO 27001 Information Classification and Risk Assessment Approach to define “borderline”

- Who should define “borderline”?
 - Answer 1: Law Makers, DPA and Enforcement Body. (Strong Law)
 - Answer 2: DPO or Compliance Officer in each company (Soft Law and Self-Co Regulation)
 - Answer 3: Expect someone and do nothing --- bad idea!
- What is ISO 27001
 - ISO 27K family - ISMS
 - Guiding Risk Assessment and Information Classification
 - Not “Prescriptive” but “Descriptive” approach to define border

No Business

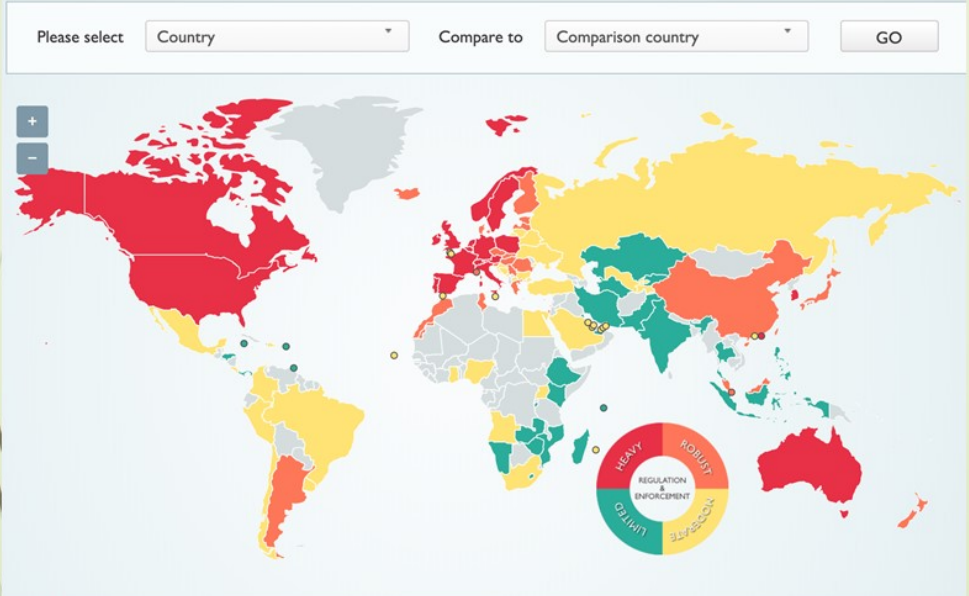


8

Panel 2 The Global Landscape for Privacy Regulation and Current Challenges

DATA PROTECTION LAWS OF THE WORLD

<https://www.dlapiperdataprotection.com/>



Comparison of National Privacy Regulations (NPR)

		EU	Japan	Hong Kong	Korea	(India)	Singapore	Philippines	(Vietnam)	Malaysia	Australia
適用範囲	域外適用	10 DPO多量露対応の必要性が不明、域外が不利	8	1	1	7	1	9	3	4	5
	民間/行政で同じ扱い	1	5	3	1	5	5	5	1	5	10
個人情報	定義	10 オンライン情報も含むと明記	7	4	7	7	9	7	7	7	9
	同意の追加的条件	10 チェックボックスですら否決	6	6	7	4	6	10	4	4	4
	子供への配慮	10	N/A	8	8	N/A	4	10	N/A	1	N/A
	無記名個人情報	9	7	1	5	6	1	9	1	4	9
DPO説明責任	DPO設置義務と役割	8	2	3	4	3	8	10	1	1	2
	プライバシー影響評価	6	3	5	6	7	7	2	7	8	2
	違反時の通知義務	10	3	3	8-10	5-8	3	10	1	1	6-8
権利保護	プライバシー通知	10	7	5	6	3	3	8	3	4	7
	アクセス権	8	3	4	6-10	6-10	5	5-10	6-10	6	2
	データポータビリティ	10	1	3	1	1	1	7	3	2	3
	忘れられる権利	10	6	2	1	1	1	8	4	2	4
	DM、プロファイリング規制	10	2	2	2	2	4	10	2	6	6
越境移転	第三国への移転の難しさ	10	3	3	8-10	5-8	3	10	1	1	6-8
法執行	罰金/懲役	9	2	6	5	3	6	7	3	5	4
	Cookieへの対応必要性	10	3	3	8	1	5	1	2	1	2

Approaches

Risk based Approach

Accountability based Approach

Inclusive Approach

Product + Data Service Convergence

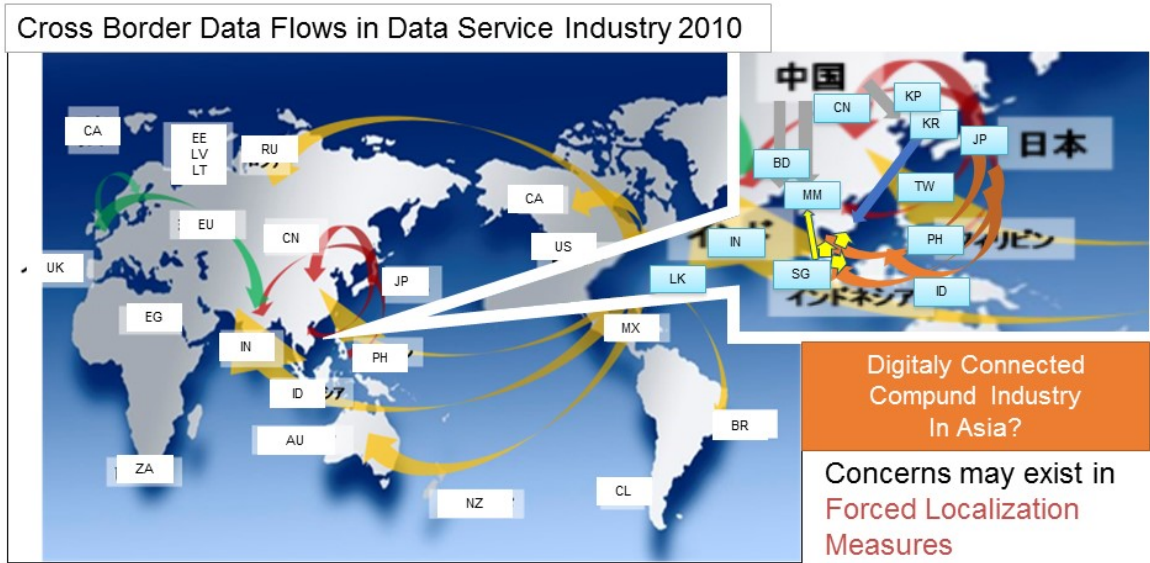


Industry Production of Things	Internet Economy Providing Value	Integration Value Added Service
Quality Control Just in Time Stock Management Automation Planning	Big Data, Small Data Public Data, Personal Data Remote Control/Maintenance 3D Printing, Remote Production	Data Driven Innovation In Asia Pacific

All Copyright Reserved 2014

11

Panel 3
Cross Border Personal Data Flows in the APEC Region



All Copyright Reserved 2014

12

12

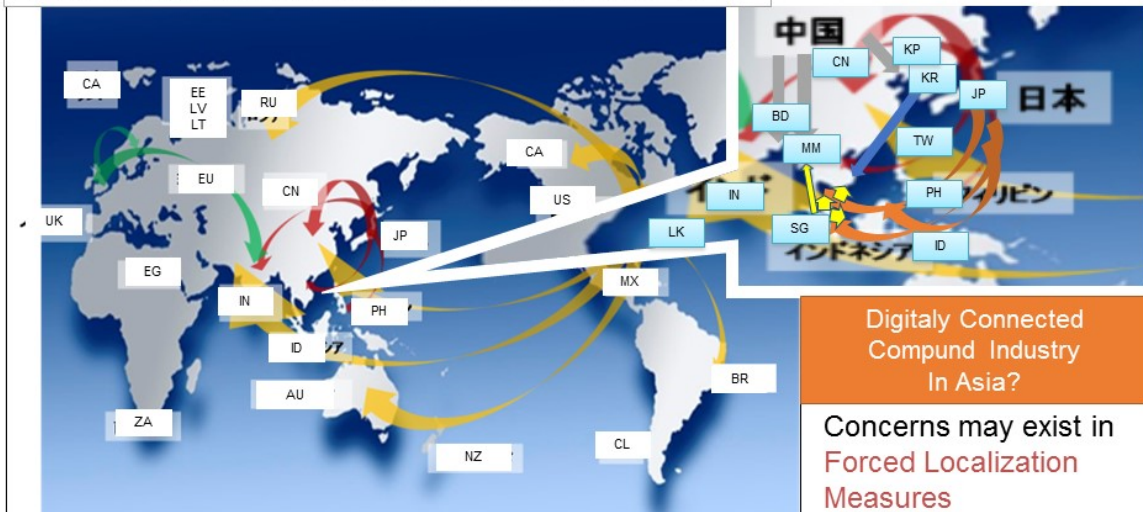
Compound/Complex vs Distributed

Question: Will each economy remain isolated in Asia?

The answer will be NO.

Market may be different, but Industry is closely connected.

Cross Border Data Flows in Data Service Industry 2010



All Copyright Reserved 2014

13

Possible Update regarding Interoperability and Benefits

The 1st CBPR Certificate In Japan



APEC Privacy Framework and GDPR are BOTH Based on OECD Privacy Guidelines in 1980/2013/2018



Interoperability



- Dual Certification with BCR, Binding Corporate Rules
- GDPR Certification Mechanisms

CBPR Benefits are SCALABLE

JAPANESE 3 CBPR Holders are Relatively Small/Medium Enterprises(MSMEs).

They all appreciate Benefits in CBPRs.

1. "Branding in Trust" Effect (B2B/B2C)
2. Risk (and Compliance Cost) Mitigation Effect
3. Network Effect and Outreach

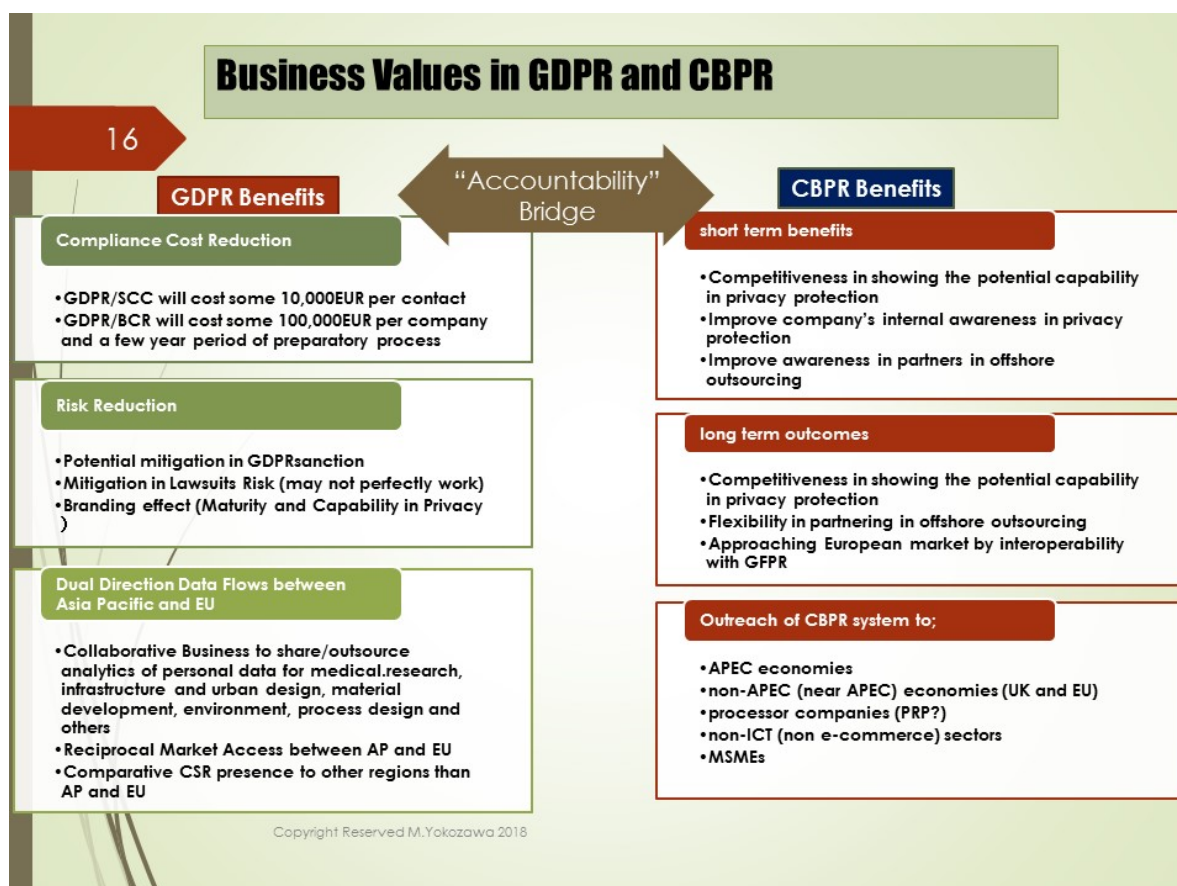
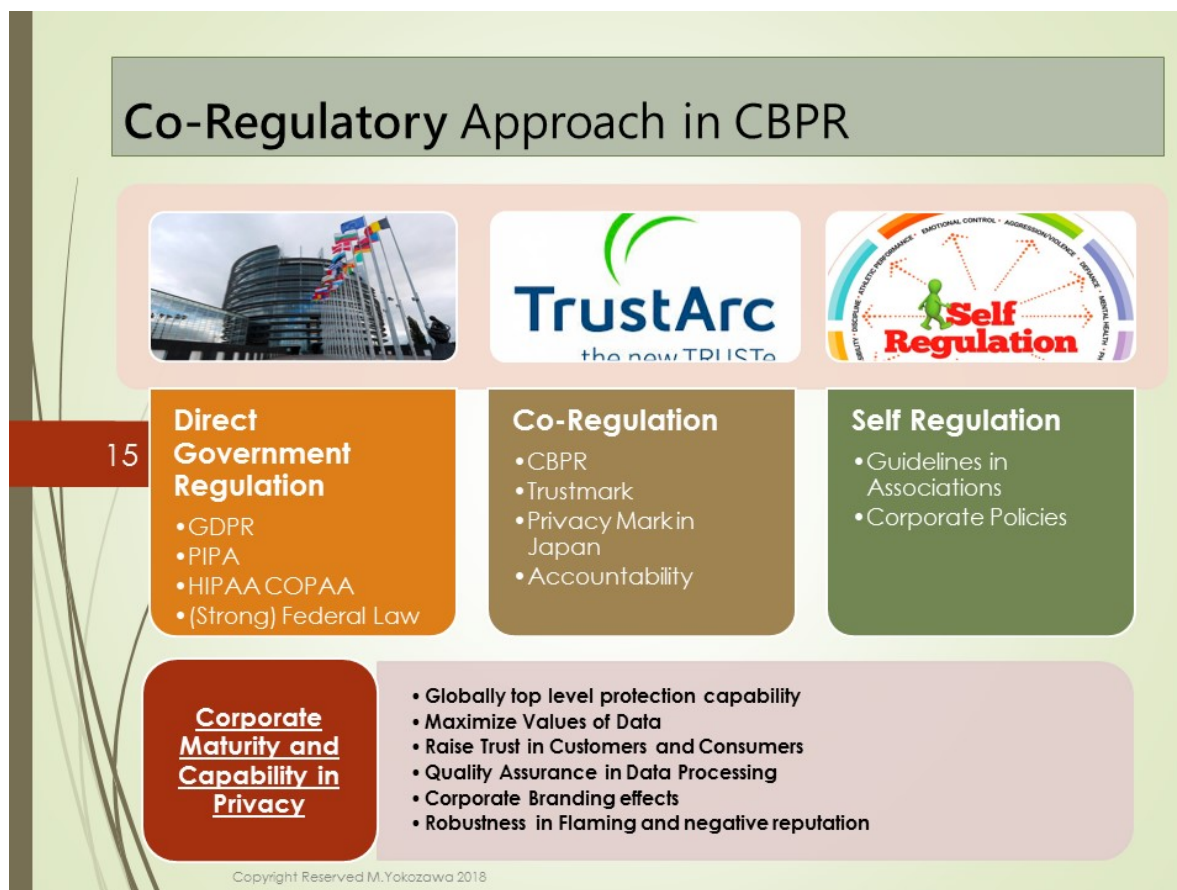
"INTASECT", the first CBPR holder in Japan appreciates that the benefit of CBPR is worth the cost

"GMO Globalsign", the second CBPR holder in Japan sees CBPR as a gateway to EU's GDPR

"PAIDY", the third CBPR holder expects legitimate outsourcing of their payment processing business to counterparts in APEC region

Copyright MOIS Research Unit, Kyoto Univ. 2019

14



E. Dr Peter Lovelock, Director, TRPC

Privacy Regulation: An Overview

APEC SOM3 | 23 August 2019 | Chile



Dr Peter Lovelock

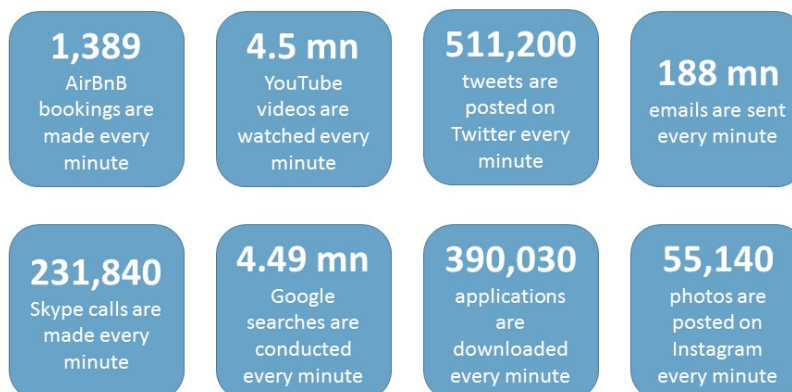
*Director and Founder | TRPC | Singapore Hong Kong
Beijing Melbourne
Associate Professor | Singapore Management University*

A Quick Roadmap

1. Introduction: Privacy in the digital age
2. Landscape of privacy frameworks
3. Challenges
4. Conclusions

Privacy in the digital age

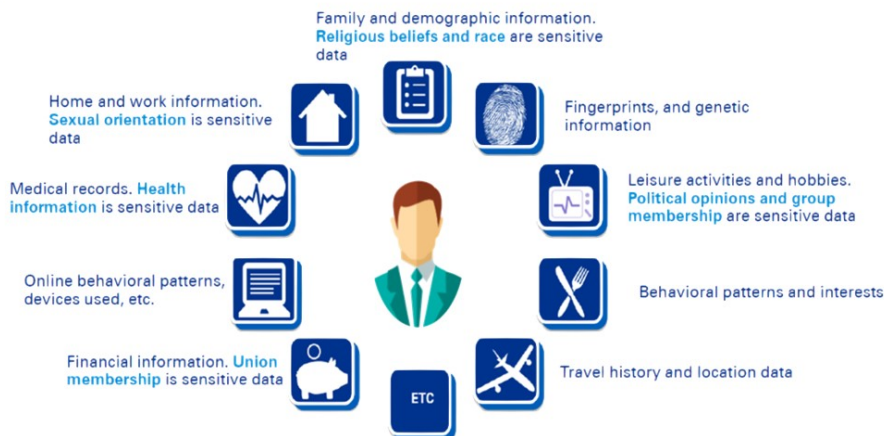
Greater connectivity increases the quantities of data being accessed, moved, and exchanged.



Source: Domo, *Data never Sleeps* 2019, www.domo.com/news/press/data-never-sleeps-7

Privacy in the digital age

The volume and the type of data circulating raise a number of legal, technical, and ethical questions.



Source: Aristi Ninja, <https://aristininja.com/personal-data-gdpr>

Privacy in the digital age

Privacy in the digital age has major financial implications.

Removing foreign digital trade barriers would increase real wages by

0.7 to 1.4%

in digitally intensive sectors.

Global data flows account for

3%

of global GDP output, the equivalent of **US\$2.3 tn.**

Unobstructed digital trade raises the GDP of the United States by

3.4 to 4.8%,

contributing to the creation of

2.4 million

new jobs.

Source:

ITC, www.usitc.gov/publications/332/pub4485.pdf

McKinsey, www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows

Brookings Institution, www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf

Landscape of privacy frameworks

Each privacy framework has its own set of priorities:

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

Source: GSMA, www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf

Landscape of privacy frameworks

Other privacy frameworks:



EU-US Privacy Shield



Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)



EU-Japan Economic Partnership Agreement



United States-Mexico-Canada Agreement (USMCA)

Source: GSMA, www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf

Landscape of privacy frameworks

Same objective, different approaches:

EU-US

- Specifically designed to protect the fundamental rights of anyone in the EU whose personal data is transferred to the United States for commercial purposes.
- Allows the free transfer of data to companies that are certified in the US under the Privacy Shield.

CPTPP

- Promotes the free flow of data across borders for service suppliers and investors as part of their business activities.
- Participants commit not to impose 'localisation requirements' that would force businesses to build data storage centres or use local computing facilities in CPTPP markets.

EU-JPN

- Postpones the provision on the "free flow of data" (Article 8.81), but provides for the processing of financial information (Article 8.63), which necessarily includes personal data.
- Facilitated the mutual recognition of domestic data protection frameworks as "equivalent".

USMCA

- Requires each economy to establish personal information protection laws, though it leaves the content of such laws and the means of enforcement to governments' own discretion.
- Contains specific data localization provisions, prohibiting requirements for data to be stored and replicated locally.



Challenges: Governments

- **Different objectives:** Data privacy regimes may collide as different economies and jurisdictions differ in the values, approaches, and outcomes they prioritise.
- **Different language:** Data privacy regimes may define basic principles and concepts in completely different manners. The bigger the scope of the regime, the more complicated it is to align legal terms such as “consent”.
- **Different journeys:** Even if fundamental principles and concepts are identical, the harmonisation and interoperability of privacy regimes may be hindered by frameworks’ different stages of maturity.



Challenges: Businesses

- **Administrative burden:** The multiplicity of privacy regimes creates complications for entities handling data of citizens in multiple jurisdictions, which may be subject to one or more regimes.
- **Financial costs:** The cost of compliance can limit small businesses’ participation in the digital economy, as they may find it more difficult to comply with broad, overarching regulations designed for bigger enterprises.
- **Economic opportunities:** Most privacy regimes are still looking to establish a balance between protecting privacy and enabling data-driven business models. Too constraining, and they limit innovation, too vague, and they create uncertainty in a fast-evolving environment.

Challenges: individuals

- **Low visibility:** The number of privacy regimes may make it very difficult for citizens and consumers to understand who is in charge of their data and what is being done to the private information they share.
- **Security concerns:** The strictness of a privacy regime does not necessarily mean it can effectively protect people's data from being stolen or leaked.
- **No recourse:** Privacy regimes are not easy to understand, so it may be a complex endeavour to know which framework applies to which individual in a given case.

Conclusions

Implications for regulators

PROMOTE INTERNATIONAL INTEROPERABILITY BETWEEN PRIVACY REGIMES

APEC economies must work together to support interoperability in data protection regimes to facilitate the secure transfer of information across borders. Most legal frameworks allow transfers to economies which provide similar protections to data. This compatibility is essential to cross-border data flows. More effective is participation in a regional data protection framework.

MAINTAIN MULTILATERAL DISCUSSIONS ON MECHANISMS TO REDUCE CROSS-BORDER DATA BARRIERS

APEC economies must urge international organisations such as the World Trade Organisation (WTO) and the World Bank to establish or enhance mechanisms to continually monitor and report on economies that introduce data localisation that will negatively impact the cross-border flow of data. Such efforts would help create an environment where businesses could develop optimal strategies when expanding internationally.

CONSIDER BILATERAL OR MULTILATERAL AGREEMENTS TO BRIDGE GAPS BETWEEN DOMESTIC PRIVACY LAWS

Bilateral and multilateral agreements that mutually recognise privacy regimes are a key approach in promoting cross-border flows while respecting particular differences in approach by each economy. Mutual Recognition Agreements (MRAs) can help bridge differences, and greatly reduce compliance processes and costs for businesses, allowing them to better focus their resources.

APEC Recommendations:



CBPR and next steps

Governments should be encouraged to join the CBPR System as soon as possible.

Setting up Accountability Agents is a business priority.

- Public education efforts should focus on reaching out to potential Accountability Agents, and capacity-building.
- A related program which could be run in tandem is a “step-up” training conducted by APEC officials and/or existing Accountability Agents, to train other possible certifying bodies to conduct the APEC CBPR assessment process.
- Multiple Accountability Agents should be certified in an economy to promote greater options and competitive pricing for the growing variety of companies seeking the benefits of a CBPR certification.
- Governments should invest in awareness building/training sessions for local businesses on the Accountability Agent model.

Recommendations and next steps



- Reduce the burden of annual certification** to a biennial certification, as the current annual re-certification process may be a deterrent to businesses joining the CBPR system.
- Publicise businesses who have been certified under the APEC CBPR**, as well as display if the certification is current.
- Professional consultancy services** should be available to assist businesses to prepare for CBPR certifications.
- Private-sector organisations that are already CBPR certified should actively work with APEC in **capacity-building efforts** to expand the adoption of the framework among member economies and companies doing business in Asia.

15

Recommendations and next steps



Create an online self-assessment for companies, leading to an Expression of Interest form.



16



TRPC

Contact:
email: peter@trpc.biz
phone: +65 6920 8561
website: trpc.biz

About TRPC:
TRPC is a boutique consulting and research firm with over 30 years experience in the telecommunications and ICT industries in the Asia-Pacific. We offer specialised advisory, research, and training services, with a focus on regulatory and strategic business issues, and possess an extensive network of industry experts and professionals throughout the region.

F. Ms Karina Kudakaeva, Researcher, Institute for International Economics and Finance, Russian Foreign Trade Academy



 RUSSIAN FOREIGN
TRADE ACADEMY

**Policy and Regulatory Environment
in Data Utilization and Protection:
the Russian Federation experience**

Puerto Varas, 2019

Outline of the Presentation

- Scope and definitions;
- Digital STRI & Russia
- Data-driven business in Russia
- Data utilization and protection policy in Russia
- Possible recommendations.



Scope and Definitions

☐ Trade in goods by electronic means

- goods, traded on e-platforms
- *electronic transmissions*

☐ Trade in services by electronic means

- ICT services - *UNCTAD approach, based on EBOPS classification.*
- digitally-deliverable services - *UNCTAD approach, based on EBOPS classification.*
- services, traded on e-platforms

☐ E-commerce related services:

- key e-platforms operators' services (software, security measures, information exchange);
- other e-platforms operators' services (advertising, dispute resolution, rating, certification, quality control, insurance, storage, transportation, delivery, electronic banking, etc.) – *UNCITRAL approach.*

Data-driven business in Russia: main statistics & trends

Digitally-deliverable services (DDS) (2017)

Export

USD 19.788 bln

+10.8% to 2016

0.7 % of global DDS export

34.2% of total Russian export

Import

USD 34.866 bln

+11.2% to 2016

1.4 % of global DDS import

39.3% of total Russian import

Source: UNCTAD

Challenges:

- Regional disproportions;
- Need for further improvement of human capital;
- Need for further development of IT-equipment and software;
- Lack of unified statistics & awareness.

Opportunities:

- ✓ Political will & support;
- ✓ Active private sector & MSMEs;
- ✓ Biggest Internet active audience in Europe – 90 mln. people;
- ✓ Well developed infrastructure (74 % coverage);
- ✓ Low prices for Internet access – 4th in the world (ITU ICT Price Basket);
- ✓ Solid human resources base;
- ✓ Competitive domestic products;
- ✓ Telecom + IT + Banks + Finance & Insurance ➔ Other services

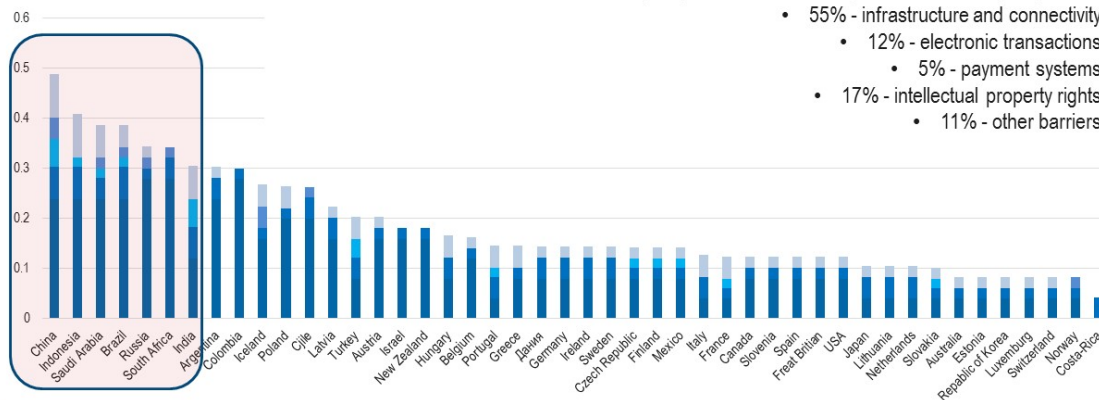


RUSSIAN FOREIGN
TRADE ACADEMY

4

Digital STRI & Russia: assessments

The Digital Services Trade Restrictiveness Index database identifies and catalogues barriers that affect trade in digitally enabled services across 46 countries.



The policy measures are categorized under five policy areas:

- 55% - infrastructure and connectivity
 - 12% - electronic transactions
 - 5% - payment systems
- 17% - intellectual property rights
 - 11% - other barriers



RUSSIAN FOREIGN
TRADE ACADEMY

■ Infrastructure and connectivity ■ Electronic transactions ■ Payment system ■ Intellectual property rights ■ Other barriers affecting trade in digitally enabled services

5

Digital STRI & Russia: assessments

I **step**: to estimate AVE of NTM in trade in services (based on Fontagne L. et al. (2011))

II **step**: to estimate the particular measures' impact in the total level of NTM (USITC approach)

	S	SA	SB	SC	SD	SE	SF	SG	SH	SI	SJ	SK
Infrastructure	-0.310	-5.452***	-1.995**	-0.367	0.452	-0.686	-0.445	-3.291***	-0.363	-1.622***	-2.556***	-0.926
Electronic transactions	-0.889	-9.918	5.366	-1.415	0.915	3.111	1.446	1.651	5.542**	-1.485	5.269*	-2.753
Electronic payments	3.638**	4.664	6.951	4.950***	6.980***	7.680*	6.827**	18.23***	1.834	6.518*	2.622	11.43***
IPR	-2.505	13.37	-5.018	-4.687***	-9.042***	-12.19**	-5.936	-9.924	5.178	7.230*	11.09**	-1.762
Other	1.712	14.22***	2.548	3.182***	3.339**	5.495*	4.013*	3.437	2.046	5.636***	0.641	2.722
Time-fixed effects	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Controls	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Number of observations	174	159	174	174	174	166	173	173	174	173	173	168

	S	SA	SB	SC	SD	SE	SF	SG	SH	SI	SJ	SK
Data localization	0.0838**	0.00176	0.0866	0.0540	0.0848	-0.103	0.290***	0.274*	0.387***	0.101	0.223**	0.289***
Time-fixed effects	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Controls	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Number of observations	174	159	174	174	174	166	173	173	174	173	173	168

* p<0.10, ** p<0.05, *** p<0.01

Abbreviation	Sector	Abbreviation	Sector
S	Services	SF	Insurance and pension
SA	Manufacturing services	SG	Financial services
SB	Maintenance and repair	SH	Charges of the use of IP
SC	Transport	SI	ICT services
SD	Travel	SJ	Other business services
SE	Construction	SK	Personal, cultural and recreational services

6

Data utilization and protection policy in Russia: personal data protection (general)

Personal Data Law, No 152-FZ, 27.07.2006;

Law on Information, Information Technologies and Information Protection, No 149-FZ, 27.07.06;

Additional orders & decrees.



New realities & challenges

Update

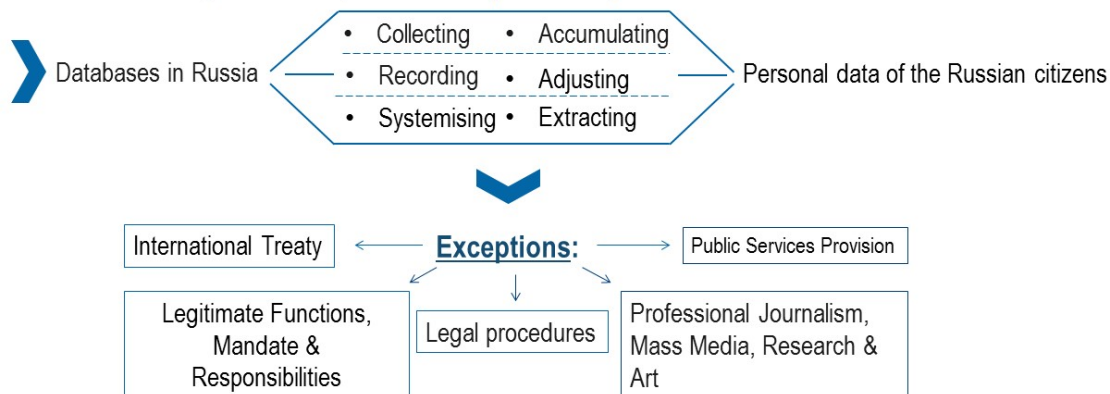
GDPR compliance



7

Data utilization and protection policy in Russia: personal data protection (localisation)

Personal Data Law, No 152-FZ, 27.07.2006 (Article 18)



Data utilization and protection policy in Russia: personal data protection (cross-border data transfer)

Personal Data Law, No 152-FZ, 27.07.2006 (Article 12)

➤ **Responsibility of the personal data operator** in insuring the legitimacy of cross-border data transfer to the third party, before conducting it.

- **Exceptions:**
- ✓ written consent for the cross-border data transfer;
 - ✓ international agreements, signed by Russia;
 - ✓ contract performance with the personal data subject;
 - ✓ important interests of the personal data subject, when it is impossible to receive a consent.

Data utilization and protection policy in Russia: personal data protection (adequacy decisions & international interoperability)

Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data No. 108, 1985



Protocol No. 223 to the Convention No. 108, 2018

- ✓ 22 economies,
- ✓ 8 from APEC (Australia, Canada, Chile, Malaysia, Korea, New Zealand, Singapore & Japan).

55 & 31 members (incl. the EU & Mexico);

- ✓ legally binding international agreement;
- ✓ common level of protection & cross-border data flows principles;
- ✓ mutual assistance (Consultative Committee);
- ✓ compliance monitoring (Supervisory Committee);
- ✓ mutual recognition with the GDPR.



List of foreign countries, which are not parties to the Convention of the Council of Europe No. 108, but provide adequate level of the personal data subjects' rights



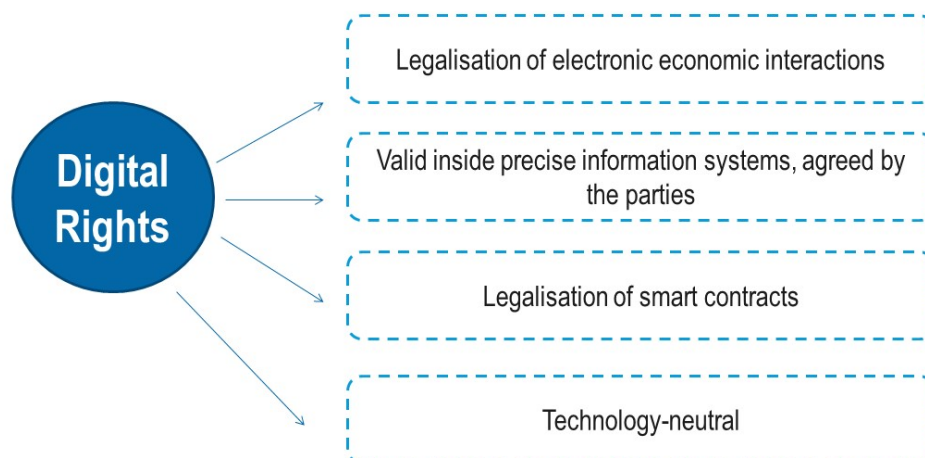
RUSSIAN FOREIGN
TRADE ACADEMY



Free flow of data to 77 economies (9 from APEC)

10

Data utilization and protection policy in Russia: new initiatives



RUSSIAN FOREIGN
TRADE ACADEMY

11

Main opportunities of the chosen policy model in Russia

SECURITY	➤	General & Information at economic, corporate & personal levels
FLEXIBILITY	➤	Legal exceptions, constant modernization
INTEROPERABILITY	➤	Convention 108 + and Adequacy decision list
FREE FLOW OF PD	➤	77 Economies, 9 from APEC
ACCOUNTABILITY	➤	Fostering new culture of communications
COMPETITION	➤	Joint ventures & New products & Integrated solutions
STANDARDS	➤	GDPR compliance



12

Thank you for your attention!

Karina Kudakaeva

Institute for International Economics and Finance
Researcher

Email: k.kudakaeva@vavt.ru
Website: <https://www.vavt-imef.ru/>
Twitter: @AnalyticsIMEF
Facebook: @TorgIMEF



13

G. Mr Alex Mauricio Pessó Stoulman, Legal, Corporate Affairs and Philanthropies Director, Microsoft Chile









Alex Pessó
Legal and Corporate Affairs Director
Microsoft Chile

Baseline Privacy Legislation

TRANSPARENCY	INDIVIDUAL EMPOWERMENT	CORPORATE RESPONSIBILITY	STRONG ENFORCEMENT
<ul style="list-style-type: none">• reasonably informed individual	<ul style="list-style-type: none">• empowered to express privacy preferences	<ul style="list-style-type: none">• data protected• documented risk assessments	<ul style="list-style-type: none">• strong regulator

Microsoft's Privacy Principles

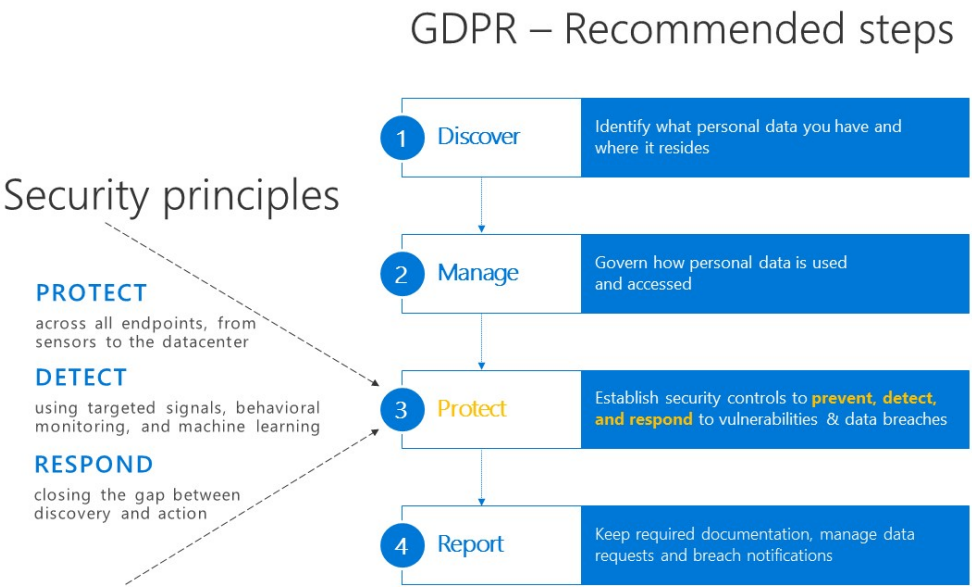
Your data, powering your experiences, controlled by you. [Microsoft Privacy](#)

Benefits to you	Control	Transparency	Security	Strong Legal Protection	No content-based targeting
					
When we do collect data, we will use it to benefit you and to make your experiences better.	We will put you in control of your privacy with easy-to-use tools and clear choices.	We will explain what we do with your data in clear, plain language.	We will implement strong security measures to safeguard your data.	We will respect your local privacy laws and fight for legal protection of your privacy as a fundamental human right.	We will not use your email, chat, files or other personal content to target ads to you.

Microsoft's GDPR Approach

	<u>Engineering investments</u> made to empower consumers, achieve compliance and help our customers achieve compliance
	<u>Real-time risk assessment.</u> Access to Compliance Manager, which empowers you to manage your compliance posture from one place.
 //privacy	<u>Privacy program & documentation</u> enhancements to achieve compliance and stand ready to face regulatory scrutiny

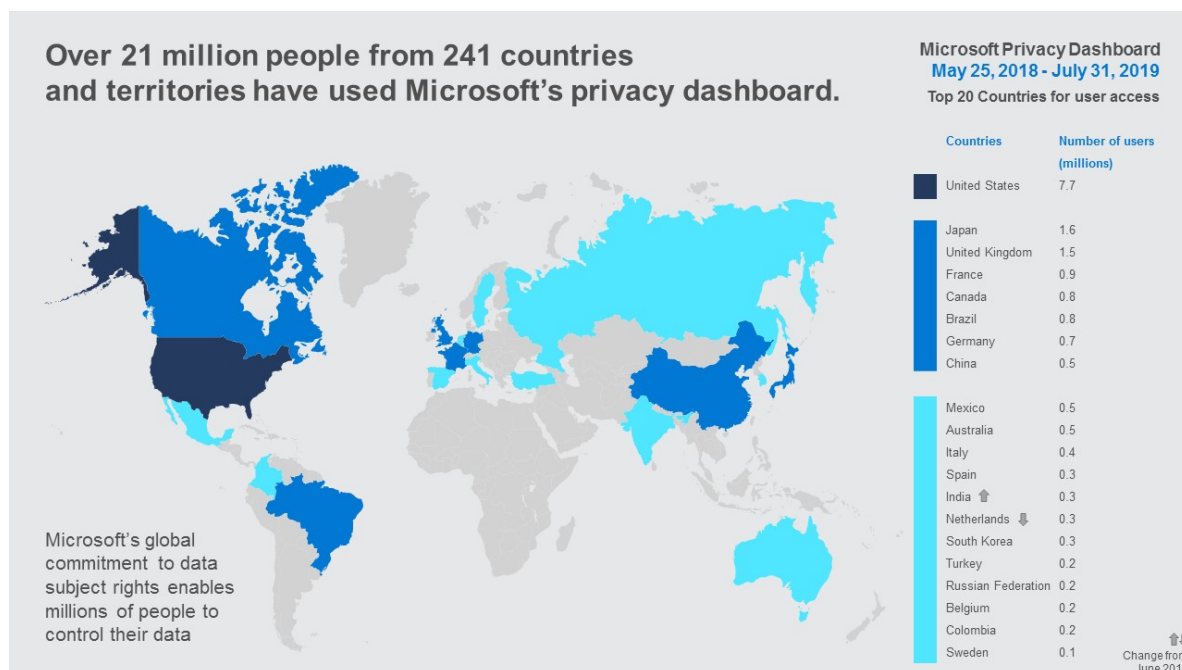




GDPR Approach



Trade Policy Dialogue on Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses



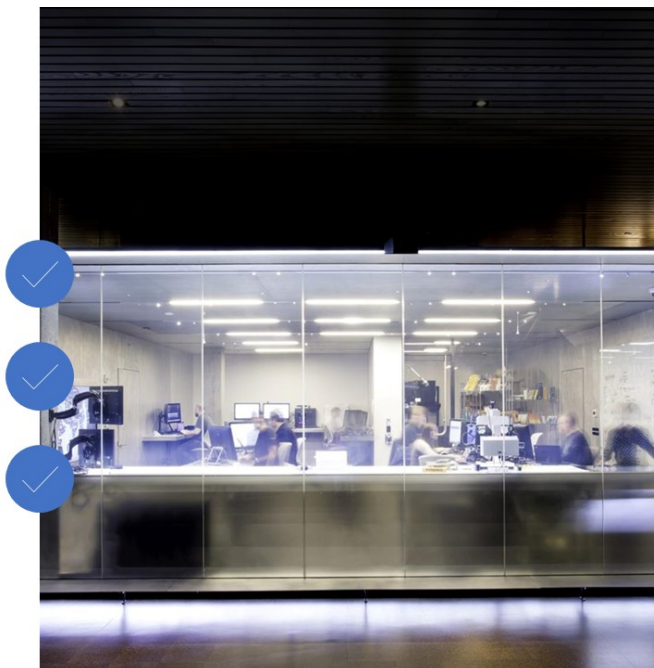
Security

We will ensure that all your data is secure

We spend over \$1 billion a year on cybersecurity.

3,500+ security professionals work to secure datacenters and hunt down attackers.

We block more than 5 billion distinct malware threats per month.



Transparency

We will be transparent about the collection and the uses of data

We provide geographic locations where customer data is stored.

We publish the number of legal demands for customer data that we receive from law enforcement agencies.

We provide visibility into what we do with customer data, how we protect it, and how they are in control.

GDPR's first anniversary: A year of progress in privacy protection

This has improved how companies handle their customers' personal data. And it has inspired a global movement that has seen countries around the world adopt new privacy laws that are modeled on GDPR. Brazil, China, India, Japan, South Korea and Thailand are among the nations that have passed new laws, proposed new legislation, or are considering changes to existing laws that will bring their privacy regulations into closer alignment with GDPR.

Get the latest on GDPR compliance >

Compliance Simplified

Control management, integrated task assignment, evidence collection, and audit-ready reporting tools to streamline your compliance workflow.

LAUNCH COMPLIANCE MANAGER >

Compliance

We will manage your data in accordance with the law of the land

We have the most comprehensive compliance coverage in the industry.

We committed to sharing our experiences in complying with complex regulations.

We make several resources available to help our customers along their Compliance journey.

Global

- ISO 27001:2013
- ISO 27017:2015
- ISO 27018:2014
- ISO 22301:2012
- ISO 9001:2015
- ISO 20000-1:2011
- SOC 1 Type 2
- SOC 2 Type 2
- SOC 3

US Gov

- FedRAMP High
- FedRAMP Moderate
- EAR
- DFARS
- DoD DISA SRG Level 5
- DoD DISA SRG Level 4
- DoD DISA SRG Level 2
- DoE 10 CFR Part 810

Industry

- PCI DSS Level 1
- GLBA
- FFIEC
- Shared Assessments
- FISC (Japan)
- APRA (Australia)

Regional

- Argentina PDPA
- Australia IRAP Unclassified
- Australia IRAP PROTECTED
- Canada Privacy Laws
- China GB 18030:2005
- China DJCP (MLPS) Level 3
- China TRUCS / CCCPF
- EN 301 549
- EU ENISA IAF
- EU Model Clauses
- EU - US Privacy Shield
- GDPR
- Germany C5

Industry

- 21 CFR Part 11 (GxP)
- MARS-E
- NHS IG Toolkit (UK)
- NEN 7510:2011 (Netherlands)
- FERPA

Regional

- Germany IT-Grundschutz workbook
- India MeitY
- Japan CS Mark Gold
- Japan My Number Act
- Netherlands BIR 2012
- New Zealand Gov CC Framework
- Singapore MTCS Level 3
- Spain ENS
- Spain DPA
- UK Cyber Essentials Plus
- UK G-Cloud
- UK PASF

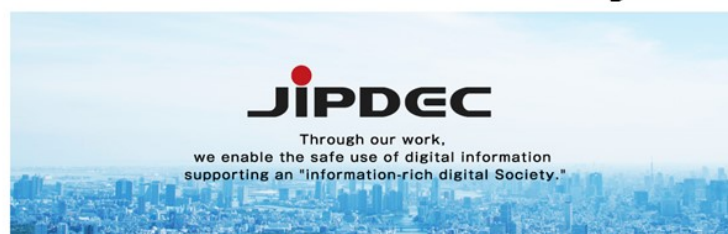
microsoft.com/en-us/trustcenter/compliance/complianceofferings

H. Mr Hiromu Yamada, JIPDEC



CBPR Accountability Agent in Japan

August 23th, 2019



We are promoting a new society...

... to create a secure and trustworthy system, and to make that system work effectively in Society, enabling a place where people can discuss issues, share their views, and work together to solve their problems.

In this digital age, our activities and creativity depend on various kinds of data. If there were a system to allow individuals, businesses, and Society to benefit from that data, a virtuous circle of data distribution would be created enabling efficient data use and sharing. Building a safe and secure data Society, we should consider the impact our activities would have on various people.

Since its establishment, JIPDEC has been collaborating with various groups across industries for the creation of a safe, convenient, and prosperous Society through the advancement of computerization. While additional industry and international cross-border collaboration are needed, we will continue to use the knowledge gained from our long history to contribute to future socio-economic activities and thus to the creation of a safer digital Society.

TOP

Accredited Personal Information Protection Organizations

About us

Our Activities

Access

<https://english.jipdec.or.jp/index.html>

About us



- Established in 1967 as Japan Information Processing and Development Center, renamed as JIPDEC in 2011.

1989 May	Published guidelines for personal data protection in the private sector(METI)
1998 Apr.	Commenced the operation of the PrivacyMark System
2016 Jan.	Became Accountability Agent
2016 Jun.	Started its operation as AA
2016 Dec.	Intasect Communications, Inc (https://intasect.com/)
2018 May	GMO GlobalSign K.K. (https://jp.globalsign.com/)
2018 Dec.	Paidy Inc. (https://paidy.com/)

Certified companies

As of Aug. 2019



2016
Dec.

Intasect Communications, Inc

(<https://intasect.com/>)



Gaining trust (proof of reliability)

2018
May

GMO GlobalSign K.K.

(<https://jp.globalsign.com/>)



Certified adequacy of cross border data transfer rules

2018
Dec.

Paidy Inc.

(<https://paidy.com/>)



Managing outsourcing companies overseas

2

CBPR Promotion (International)



Title	Place	Host	Date
Public-Private Dialogue session before ECSG	Ho Chi Minh	VNM	Aug 2017
Side event of 39th ICDPPC	Hong Kong	PPC	Sep 2017
CBPR seminar (Capacity Building)	Taipei	TPE	Oct 2017
CBPR seminar (Capacity Building)	Manila	PHL	Dec 2017
AA PreMeeting	Tokyo	TrustArc JIPDEC	May 2018
Privacy Perspectives from the Asia-Pacific	Brussels ICDPPC	C&M International	Oct 2018
JISA/ASOCIODigital Masters Summit 2018	Tokyo	JISA/ASOCIO	Nov 2018
Thailand and Japan Digital Governance seminar	Bangkok	ATCI	Dec 2018

3

CBPR Promotion (Japan)



Title	Place	sponsor	Speaker	Date
CBPR seminar	Tokyo	METI	METI, PPC, DoC(US) JIPDEC IntaSect	Oct 2016
APEC/CBPR roundtable	Tokyo	CiPL	METI, PPC, DoC(US) KOR, TPE JIPDEC	May 2017
APPA Privacy Awareness Week symposium	Tokyo	ACCJ	PPC, CiPL, JIPDEC	May 2018
CBPR seminar	Tokyo	METI JIPDEC	METI, PPC, DoC(US), JIPDEC , GMO GlobalSign	May 2018

4



Thank you for your attention!



5

60