[Draft as of 2023-07-24]

Toward Freer Safe and Trusted Flow of Data in the Asia-Pacific Region

Insights from Two Roundtables

22 February 2023, Institute of International Finance, Washington DC, USA
25 April 2023, Singapore Business Federation, Singapore

In 2019, the APEC Business Advisory Council (ABAC) proposed an *APEC Roadmap for a New Financial Services Data Ecosystem*,[1] which was welcomed by the APEC Finance Ministers at their annual meeting that year. The Roadmap, which was developed by the Asia-Pacific Financial Forum (APFF) through a series of conferences in Singapore, Washington DC, Beijing and Atlanta and consultations with APEC finance officials in Chile and ASEAN+3 officials and regulators at the Asian Development Bank (ADB) in Manila, outlined pathways for a regional approach to expanding safe and trusted cross-border data flows among APEC member economies, in addition to good practices in developing domestic ecosystems for inclusive and robust data collection, sharing and use.

Among the recommendations in the Roadmap were regional collaboration to identify measures toward achieving inter-operability of privacy regimes across jurisdictions (in addition to the APEC Cross-Border Privacy Rules) and identifying privacy-enhancing technologies (PETs) that could be used to expand cross-border data sharing in compliance with privacy laws and regulations. Considering the huge amount of work that had been undertaken since then on these two issues in various fora within the region and all over the world and the significant advances in PETs, ABAC and APFF are seeking this year to update the approaches outlined in the 2019 Roadmap and develop new recommendations for consideration by relevant groups within APEC to incorporate in their respective work plans.

In pursuit of this goal, ABAC and the APFF Data Ecosystem Working Group are collaborating with leading international organizations and stakeholders from industry, the legal community and the public sector to undertake discussions through roundtables on both sides of the Pacific in the first half of 2023. This Roundtable held in Washington DC aimed to discuss innovative and practical approaches to privacy protection in cross-border data sharing, the opportunities arising from advances in PETs and the role that government policy and regulation and APEC collaboration can play in enabling the expanded safe and trusted cross-border flow of data in the region.

Implementation of Cross-Border Data Flows: Challenges and Opportunities

The global economy stands to benefit from the expanded flow of data, wherever it is enabled by regulatory frameworks. For financial services, which play a key role in global trade and investment, data free flow with trust is particularly important. The financial services sector,

[1] https://www2.abaconline.org/assets/2018/APFF/Data_Ecosystem_Roadmap_Final.pdf

which has become one of the most digitalized and globalized sectors, is reliant on cross-border data flows as financial transactions have become data transfers, market infrastructures such as stock exchanges and payment systems have become data networks and financial institutions have become data processors that gather, analyze and trade customer data.[2]

Current regulations in many cases have not recognized this reality. For example, the concept of data portability does not take into account reciprocal data sharing in the open banking context. Also, separate regulations for personal data, personal financial data, financial regulatory records and important data do not take into account that these tend to be intertwined. Handling them holistically would enable banks to improve products and services, risk management, prevention of financial crime and meet customer needs for more tailored and personalized services.[3]

The issue of cross-border data flows arising from differences in regulatory requirements is becoming ever more critical for financial inclusion, particularly with respect to cross-border payments and credit history, as more and more people move from one jurisdiction to another as businesspersons, tourists, immigrant workers or refugees. Cross-border data transfers for critical use cases such as digital identity verification and authentication and artificial intelligence applications through an array of tools are facing complex standards for verification and harmonization that hinder the ability to verify access across jurisdictions to facilitate onboarding and data collection.

The main barrier to data flows is not the lack of tools but the complexity of legal frameworks. This is true even in domestic contexts where there are several levels of government, such as in the USA, where the approach to data privacy is currently fragmented. While there has been growing consensus on principles, policymaking and regulations are being driven at the state instead of the federal level, where mechanisms such as the issuance of rules by the Federal Trade Commission can be challenged in courts. This fragmentation also poses a huge challenge for businesses with respect to cross-border data transfers.

In the international context, businesses will continue to face difficulties unless data protection across jurisdictions is resolved. A key issue affecting cross-border data flows today is data localization, which has seen a growing trend of adoption in many jurisdictions, doubling in number over the four years from 2017 (67 measures in 35 economies) to 2021 (144 measures in 62 economies), according to a study by the Information Technology and Innovation Foundation (ITIF). [4] The same study provides estimates of the economic impact of data

---

[2] Douglas Arner, Giuliano Castellano, Eriks Selga, Financial Data Governance: The Datafication of Finance, the Rise of Open Banking and the End of the Data Centralization Paradigm (February 2022) [https://hub.hku.hk/bitstream/10722/311588/1/content.pdf?accept=1]

[3] IRSG, The future of international data transfers (April 2022) [https://irsg.co.uk/publications/irsg-report-the-future-of-international-data-transfers/]

[4] Data localization is described as involving: (a) restrictions on the transfer of particular types of data outside the borders of a jurisdiction; (b) restrictions based on broad categories such as data classified as sensitive, important, core or related to a jurisdiction's security; or (c) making data transfers too complicated, costly and uncertain for firms (de facto localization). Five different types of rules used to enforce data requirements include: (a) local data mirroring (requirement for firms to store a copy – in cases the most updated version – of data locally before being allowed to transfer a copy outside the jurisdiction);(b) explicit local data storage (requirement to physically locate data in the jurisdiction of origin); (c) de facto local storage and

localization – a one-point increase in data restrictiveness can reduce an economy's gross trade output by 7 percent, slow its productivity by 2.9 percent and cut downstream prices by 1.5 percent over five years.

Various reasons for data localization in different jurisdictions have been given. The ITIF study observed five rationales for data localization: (a) data privacy, protection and cybersecurity; (b) digital protectionism subsumed under the concept of data sovereignty for the development of local firms; (c) censorship and surveillance for purposes of protecting public interest and political/social stability; (d) law enforcement and regulatory oversight; and (e) response to and insurance against geopolitical risks, including financial sanctions.

A number of studies have concluded that data localization is not an effective response to the concerns that have given rise to such measures. A study by the International Regulatory Strategy Group (IRSG)[5] for example concludes that: (a) data localization does not result in better data security as it leads to the hosting of data in multiple less sophisticated and more vulnerable environments instead of in centralized data centers that allow for more significant investment in security measures; (b) it prevents full regulatory oversight when financial products and services are transacted across borders; (c) it increases compliance costs and thus reduces investment, impacting the local economy and businesses; and (d) it negatively affects local businesses and markets by impacting the ability of smaller businesses to make use of cloud data storage in technologically sophisticated jurisdictions to ensure data security, as well as the activities of international businesses that regularly transfer personal data across borders.[6]

Data adequacy across economies would be the ideal solution, but it is currently difficult to achieve due to the inherent inefficiency in its application, as demonstrated by the limited number of jurisdictions that have succeeded in concluding adequacy arrangements with the EU.[7] Mutual adequacy agreements require a lot of complex work and pre-requisites that are impractical for many jurisdictions to address in the foreseeable future. A major fundamental tension impacting cross-border data transfers today is the evolving relationship between the EU and the USA, whose economic partnership has been the single most important driver of global

---

processing (strict requirements such as pre-approvals for transfers and explicit consent and uncertain legality of data transfers combined with steep fines and arbitrary enforcement); (d) explicit prohibition of data transfers outside the jurisdiction; and (e) explicit local and discriminatory data processing, routing and storage, including discriminatory licensing, certification and other restrictions on foreign firms in managing and processing local data. Nigel Cory and Luke Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them* (Information Technology & Innovation Foundation, July 2021). [https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/].

[5] The IRSG is a practitioner-led body based in the UK comprising leading representatives from the financial and professional services industry, aiming to be a leading cross-sectoral group in Europe for the financial and related professional services industries to discuss and act upon regulatory developments. [https://www.irsg.co.uk/]

[6] IRSG, How the trend towards data localization is impacting the financial services sector (December 2020) [https://www.irsg.co.uk/publications/irsg-report-how-the-trend-towards-data-localisation-is-impacting-the-financial-services-sector/]

[7] Currently, these include Andorra, Argentina, Canada (commercial organizations under its Personal Information Protection and Electronic Documents or PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, United Kingdom and Uruguay.

economic growth, with both together accounting for 42 percent of both global GDP and global trade in goods and services. Within the Asia-Pacific region, the lack of coordination in the introduction of new privacy laws and regulations is seriously impacting businesses' ability to expand cross-border trade and investment, with MSMEs that, unlike larger companies, do not have the resources to navigate through different laws, definitions and sectoral regulations applying to the same sets of data, most affected.

Policy and Regulatory Innovation

Without any consensus for the moment on more flexible ways to achieve data adequacy, such as the use of the privacy shield approach,[8] the region will need to develop practical interim solutions that could enable firms to conduct business operations that require transferring data across borders with an adequate level of legal certainty and compliance with regulatory standards. Indeed, while there is currently no "silver bullet" that can provide a comprehensive and definitive solution there is scope for the use of a toolbox of mechanisms to enable the expansion of cross-border data flows. These include business-level mechanisms such as the following[9]:

- Contractual safeguards: Regulators could agree to a set of contractual data privacy and security controls that are compatible across jurisdictions, allowing for flexible implementation. Clauses will need to be sufficiently detailed, and common approaches developed to provisions for recourse of individuals whose data are transferred.
- Binding corporate rules (BCRs): Authorities could develop common procedural and administrative rules (e.g., prior regulatory authorization) based on assessment of BCRs' strengths and limitations in the Asia-Pacific context and the demand for this mechanism among companies operating in the region.
- Certification: Regulators could develop common criteria for certification and accreditation of certification bodies to promote convergence of certification mechanisms across jurisdictions that would enable organizations to demonstrate their adoption of safeguards that would be compliant with personal data protection frameworks across the region. This could build on certification schemes that are already in place within the region such as in Japan, the Republic of Korea and Singapore.

[8] The 2016 EU-US Privacy Shield was based on 7 main principles: (a) notice (individuals must be informed of the collection and use of their data and how they can contact the organization with any inquiries or complaints); (b) choice (individuals can opt out of the collection and forward transfer of the data); (c) accountability for onward transfer (transfers allowed only to third parties following adequate data protection principles); (d) security (reasonable efforts needed to prevent loss of collected information); (e) data integrity and purpose limitation (data must be relevant and reliable for the purpose of collection); (f) access (individuals must be able to access information held about them, and correct or delete any inaccuracies); and (g) resources, enforcement and liability (mechanisms to enforce rules must be in place) [https://www.privacyshield.gov/article?id=Requirements-of-Participation]. It was struck down by the European Court of Justice in 2020 (the *Schrems II* decision) on the grounds that it did not provide adequate protections to EU citizens from government surveillance.

[9] Asian Business Law Institute, *Transferring Personal Data in Asia: A path to legal certainty and regional convergence* (May 2020).

- Codes of Conduct or Privacy Codes: Jurisdictions could allow organizations to transfer data to overseas organizations that adhere to a locally approved Code of Conduct or Privacy Code. This would require the Code to be legally binding and a contract between organizations transferring data across borders to be concluded to ensure application and enforcement of the safeguards of the Code, especially those concerning the rights of data subjects, in the receiving jurisdiction. In addition, this would also require agreement among jurisdictions on the criteria for approval of Codes, how the Codes may be considered legally binding in multiple jurisdictions, appropriate recourse mechanisms for individuals in the event of breaches happening overseas, and criteria for accrediting monitoring bodies to ensure compliance with the Code, among others.
- Exemptions: Jurisdictions could work toward harmonization of existing statutory exemptions or derogations from the main rule applicable to data transfers to allow the same approach to be used in the same set of circumstances across the region. While this approach may not be practically applicable in matters of sovereignty, exemptions in more neutral areas could be achievable. Commonly agreed rules of interpretation would be needed to ensure that exemptions are narrowly interpreted and do not end up becoming the rule.
- Administrative exemptions: Jurisdictions could work together to harmonize the conditions for granting individual exemptions from compliance with data transfer rules that are granted upon request in certain jurisdictions.
- Wider participation in the APEC Cross-Border Privacy Rules (CBPR): Participation of more economies as well as organizations would help CBPR achieve a network effect and facilitate its use to enable expanded data transfers across the region.

The uncertainties arising from data localization, particularly in jurisdictions where sweeping obligations apply and where regulations are in constant flux, may be practically addressed through various means. These could include, for example, putting rules in place requiring common and consistent standards for localization requirements as applied to different sectors; clarifying the interplay between transfer provisions in general data protection laws and localization requirements mandated by specific sectoral laws or regulations; and clarifying the scope of localization measures (e.g., distinguishing between data and data sets and capturing the context within which the same personal information may be considered sensitive or not), the conditions under which exemptions are permitted and regulatory expectations in the implementation of localization rules for specific categories of data.

Several initiatives that seek to improve the current situation are worth mentioning:

- The first, if eventually translated into legal documents, is the Trans-Atlantic Data Privacy Framework. Being developed to replace the previous Privacy Shield legislation invalidated by the EU court in 2020, it provides an approach that may be considered as a model for arrangements between jurisdictions. This protocol between the U.S. and the EU would allow data to flow freely and safely between the two regions. It aims to provide better privacy protection and limit U.S. intelligence access to EU residents' data. It would also enable EU residents to seek redress through an independent court. Companies that process

data transferred from the EU have to self-certify their adherence to the principles of the framework.

- The second is regional cooperation within ASEAN. From a commercial perspective, the region has been moving in the right direction through harmonization efforts, especially among developing economies. Southeast Asia has moved ahead with its own 2016 ASEAN Framework on Personal Data Protection,[10] the ASEAN Framework on Digital Data Governance, the 2019 ASEAN Data Protection and Privacy Forum, and its 2021 ASEAN Digital Masterplan, ASEAN Data Management Framework and ASEAN Model Contractual Clauses for Cross Border Data Flows (MCCs).[11] These efforts form key elements of ASEAN's drive to achieve seamless cross-border payments through the harmonization and modernization of its member economies' payments infrastructure, together with efforts in related areas such as cybersecurity, online dispute resolution and consumer protection for e-commerce.
- The third is the work of the OECD. The recent OECD Declaration on Government Access to Personal Data Held by Private Sector Entities[12] clarifies how domestic security and law enforcement agencies can access personal data under existing legal frameworks. This work aimed to address concerns related to unconstrained and disproportionate government access to personal data held by the private sector, which has become a crucial issue for data governance and protection of individual rights and as a potential barrier to trusted cross-border data flows.
- A fourth is the ASEAN Banking Interoperable Data Framework (IDF), which is a private sector initiative of the ASEAN Bankers' Association (ABA). The IDF is a voluntary and non-binding principles-based framework that aims to facilitate the integration and use of digitalized data by banks across ASEAN member economies and to leverage governance and technology to streamline cross-border data sharing. It is envisioned to drive cross-border projects such as enabling a regional multilateral payment system[13] and enhancing risk management through greater oversight of credit risk.[14] It provides guidance that has incorporated the latest regulatory and legal requirements and various recommended practices[15] at the time of its

---

[10] https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf

[11] https://asean.org/wp-content/uploads/2021/08/ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows.pdf

[12] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

[13] By anchoring the scope on business needs and surfacing key data protection requirement, the IDF can assist in navigating through many local regulatory requirements and provide greater clarity on governance of data handled by multiple stakeholders.

[14] By helping identify opportunities from reviewing data localization laws to streamline the data sharing process, IDF can minimize credit risk exposure arising from long lead times of up to 2 months for credit risk updates,

[15] These include (a) industry practices from Enterprise Data Management Council's framework on controls for the management and protection of sensitive data in the cloud; (b) best practices from the World Economic Forum's Cross-Border Data Collaboration Roadmap; (c) practices from the ASEAN Data Management Framework; (d) local member economies' data collaboration frameworks where applicable; and (e) ISO 270001 prescribing standard practices for protection and governance of data security. ASEAN Bankers' Association, ASEAN Banking Interoperable Data Framework (IDF): Safe and secured cross-border flow of data. Guidance Document [http://www.aseanbankers.org/ABAWeb/files/Resources/ASEAN%20Banking%20IDF/ASEAN_Banking_Interoperable_Data_Framework_Guidance_Document_Version_1_0.pdf]

publication on whom data may be shared with, the types of data to be shared, how they may be shared and the binding conditions for such sharing. Its key underpinning components are legal and regulatory compliance, technology and advocacy and has six foundational components: governance and oversight, policies and procedural documents, data inventory, impact/risk assessment, controls and monitoring/continuous improvement.

Given the impact of privacy rules on digital technologies, it is important to design policies in a way that facilitates the future growth of the digital economy by understanding technologies first before introducing regulations. One example is artificial intelligence (AI), which is predicted to contribute as much as USD 15 trillion to the global economy over the next five years, benefiting a wide range of sectors from industry to agriculture to insurance in many Asia-Pacific economies. Effective AI requires highly integrated technologies to facilitate the exchange and use of customer data, particularly for e-commerce companies. However, the use of AI could face a costly and complex process in meeting privacy standards as currently designed. Work is currently ongoing on regulatory frameworks governing AI in the EU (the Artificial Intelligence Act), in Canada (the Artificial Intelligence and Data Act or AIDA) and in the USA (the AI Bill of Rights).

Stakeholders come from different regions and settings, with varying levels of understanding and technical gaps. This calls for cross-border and cross-sectoral cooperation. Public-private dialogue is important to ensure that regulation does not stifle innovation, especially in design of risk-based approaches that proportionately take into account the significance of particular transactions, as well providing tools to enable not just transparency but also traceability, which involves more granular data.

More inclusive dialogue is important to correctly identify and manage risk, ensure that resources are focused on outcomes rather than mere compliance, facilitate the adoption of the best technologies and anticipate future use cases. Particularly important is the involvement in the dialogue of the banking industry, which is seen by most consumers as the trusted custodian of their customer data. Conversations about data flows also need to include, in addition to government and business stakeholders, the technical-level people who have subject matter expertise that can help identify solutions to key issues such as matching of data, purposes of transfer and safeguards.

An important recommendation from industry is that policymakers advance the mutual recognition of core principles to protect both personal and non-personal data while ensuring cross-border opportunities. These core principles[16] include:

- Principles-based approach to data protection: Standards and safeguards (based on principles set out in Part 2 of the OECD Guidelines[17]) that can be mutually recognized

[16] IRSG, How the trend towards data localization is impacting the financial services sector (December 2020) [https://www.irsg.co.uk/publications/irsg-report-how-the-trend-towards-data-localisation-is-impacting-the-financial-services-sector/]

[17] https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

multilaterally across legal jurisdictions, providing assurance that data will be sufficiently protected when transferred.

- Addressing regulatory oversight concerns by rules of access instead of location: Control over, access to and responsibility for data should remain with the local regulated entity, which should be legally documented in the contract with the outsourcing provider.
- Focus of operational resilience should be the quality of the outsourcing solution and not its location: Operational resilience should be assessed based on a qualitative analysis of data protection measures instead of location of outsourcing service provider.
- Enhanced international cooperation: Regulators in different jurisdictions should cooperate such as through memoranda of understanding to ensure appropriate and proportionate access to data irrespective of location.
- Removing barriers through international trade agreements: Modern and forward-looking trade agreement provisions allowing the free flow of data without any requirement for localization as a condition for doing business (e.g., as in the UK-Japan Comprehensive Economic Partnership Agreement) should be considered.

It must be borne in mind that complex legal frameworks, while useful in the current context, are not the ideal solution, as they create compliance silos that may increase compliance costs and information security risks as well as force organizations to maintain large compliance teams and back-office structures. While large companies have resources to deal with this challenge, MSMEs will struggle to meet these compliance demands. Ultimately, economies need to aspire to constructing a strong culture of data protection across jurisdictions and consistent regulatory frameworks that are responsive to the needs of the market rather than the theory.[18]

Privacy-Enhancing Technologies

The potential of privacy-enhancing technologies (PETs) as pragmatic digital solutions that can complement privacy and data protection laws and regulations by enabling the processing of data in ways that comply with these rules is widely recognized in key jurisdictions.[19] The EU's General Data Protection Regulation (GDPR) acknowledges the use of PETs in a way that can meet its requirements.[20] Other references exist in Article 3(7) of Korea's Personal Information

[18] IRSG, The future of international data transfers (April 2022) [https://irsg.co.uk/publications/irsg-report-the-future-of-international-data-transfers/]

[19] The Communiqué Roundtable of the G7 Data Protection and Privacy Authorities dated 8 September 2022 states: "Privacy-enhancing technologies (PETs) – such as trusted research environments, federated learning, differential privacy, zero knowledge proofs, secure multiparty computation and homomorphic encryption – help organizations implement or improve data protection by design through processes which mask or transform personal data to reduce its identifiability…The use of PETs can facilitate safe, lawful and economically valuable data sharing that may otherwise not be possible, unlocking significant benefits to innovators, governments and the wider public. In recognition of these benefits we, as the G7 data protection and privacy authorities, will seek to promote the responsible and innovative use of PETs to facilitate data sharing, supported by appropriate technical and organizational measures." [https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Kurzmeldungen/G7-Communique.pdf?__blob=publicationFile&v=3]

[20] Article 25 refers to the implementation of "appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate

Protection Act, the Australian Privacy Principle (APP) 11 and Article 16 of Mexico's General Data Law. France's *Commission Nationale de l'Informatique et des Libertés* (CNIL), an independent French administrative regulatory body whose mission is to ensure that data privacy law is applied with respect to personal data, has a statutory duty to promote the use of PETs.

There has been increasing interest in PETs on the part of governments, in particular to understand their value and limitations. In December 2022, the U.S.-E.U Trade and Technology Council announced their upcoming assessment of the use of PETs, particularly in the health sector.[21] In 2022, the White House Office of Science and Technology Policy (OSTP) solicited public input on how to responsibly advance and adopt PETs in the United States in a manner that equitably benefits individuals and society.[22]

The OECD 2013 Privacy Guidelines recommended that member economies consider the promotion of technical measures that help to protect privacy and its 2021 Recommendation on Enhancing Access to and Sharing of Data specifically called for fostering the use of PETs. PETs have a useful role to play in helping organizations comply with privacy protection principles. An OECD analysis concludes that PETs can benefit organizations in implementing several of its privacy principles, particularly those that refer to international application, security safeguards, collection limitation, use limitation, individual participation and accountability.

Modern businesses can greatly benefit from the use of PETs. For example, conglomerates that operate in a wide variety of industries and share and use large volumes of data for different purposes, whether as storefronts, exchanges or marketplaces[23] could benefit from a platform that can enable secure data exchange and collaboration within their respective data ecosystems. A platform that is able to democratize data to develop high-value data products and innovative solutions, create ecosystems to unlock possibilities and forge synergies across industries, provide scalable data science capability to drive commercial outcomes throughout the group, and leverage data exchange to commercialize data science services across markets can increase operational efficiency, strengthen risk management and optimize business revenues. Technology is critical for data governance (control over which users will have access to a particular data set), technical security and risk management that ensure compliance with legal and regulatory requirements for data protection in markets where these companies operate.

---

the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."

[21] https://www.whitehouse.gov/ostp/news-updates/2022/07/20/u-s-and-u-k-launch-innovation-prize-challenges-in-privacy-enhancing-technologies-to-tackle-financial-crime-and-public-health-emergencies/

[22] https://www.whitehouse.gov/ostp/news-updates/2022/06/28/advancing-a-vision-for-privacy-enhancing-technologies/

[23] A **storefront** involves a one-way interaction between a single supplier and multiple isolated customers, as in the case of a large financial services data vendor supplying data directly to customers to accelerate sales and reduce costs. An **exchange** involves two-way supplier/consumer interaction with multiple isolated organizations, for example, when a large real estate data vendor collaborates directly with customers who bring their own data and consume data and models. A **marketplace** involves a one- or two-way interaction among multiple organizations, such as when a large conglomerate enables multi-party data access and collaboration among multiple legal entities to generate high-value insights. Source: *Aboitiz Data Innovation*.

The PETs space is rapidly evolving. They are at various stages of maturity, and while some are already being used widely, others are still to become operational. There are various categories of PETs with different use cases.[24] These include:

- Data obfuscation tools, such as those used for:
  - anonymization (conversion of personal data into data that cannot identify any particular individual);
  - differential privacy (injecting of randomized noise to datasets while still allowing statistical analysis);
  - zero knowledge proofs(protocols for proving to another party the possession of information that the other party does not have); and
  - synthetic data generation (creation of artificial data with the same statistical properties of the real data).
- Distributed data processing tools, such as those for:
  - federated learning (training of machine learning models at multiple decentralized devices and services and combining insights into a single global model without having to share training data);and
  - distributed analytics (enabling software and statistical analysis programs from multiple nodes to access data residing in a central location with the data controller).
- Data accountability tools, such as:
  - accountable system (software systems that manage the use and sharing of data and track compliance),
  - personal data stores (personal information management sytems that give control of personal data storage to individuals who can choose where and how they want their data stored, accessed or processed), and
  - threshold secret sharing or multiparty computation threshold signing (cryptographic tool requiring a predetermined number of keys held by different key holders to unlock encrypted data).
- Encrypted data processing tools, such as:
  - homomorphic encryption (enabling computational operations to be done with encrypted data without the need for decryption);
  - secure multi-party computation or SMPC (protocol that enables joint processing on distributed nodes without the need to share data);
  - private set intersection(a form of SMPC that reveals only the shared elements across the different datasets); and
  - trusted execution environments (secure area in a device's central processing unit that allows the running of code and access to data in an isolated manner).

Being at an early stage of development, PETs face a number of challenges. These include insufficient understanding by many regulators and consequently the lack of clear guidance that

[24] Future of Privacy Forum, *Privacy 2020: 10 Privacy Risks and 10 Privacy Enhancing Technologies to Watch in the Next Decade* [https://fpf.org/wp-content/uploads/2020/01/FPF_Privacy2020_WhitePaper.pdf]; and OECD (2023), "Emerging privacy-enhancing technologies: Current regulatory and policy approaches", *OECD Digital Economy Papers*, No. 351, OECD Publishing, Paris [https://doi.org/10.1787/bf121be4-en].

can provide certainty to businesses that the use of particular technologies are compliant with privacy requirements in their jurisdictions, which in turn hinders investment given the high cost of implementation in terms of effort, time and resources and the development of talent. Each technology has its benefits and drawbacks and degree of usefulness in bridging the privacy-utility trade-off.

There are various ways by which governments can foster innovation in relation to PETs:

- Research and development: The US' official strategy for privacy preserving data sharing and analytics aims to foster R&D to help researchers, physicians and others gain better insights from sensitive data without the need for data access.
- Secure data processing platforms: In the United Kingdom, OpenSAFELY was developed as a secure analytics platform in response to the COVID-19 pandemic.
- Certification of trusted PETs: In Japan, the Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade and Industry (METI) formulated guidelines for the certification of personal data trust banks that are used by private organizations such as the Information Technology Federation of Japan.
- Innovation contest: In France, the CNIL together with the French National Institute for Research in Digital Science and Technology (Inria) have been giving since 2016 the CNIL-Inria Privacy Award to scientists and researchers in order to encourage research on PETs. Similar initiatives are also being sponsored by the UK and USA.
- Regulatory sandboxes: In Singapore, the Infocomm Media Development Authority (IMDA) and the Personal Data Protection Commission (PDPC) launched in 2022 a PETs sandbox aiming to provide a safe environment and testing ground for pilot PET projects, with participation from the financial industry
- Digital identity management: In Finland, policymakers are developing domestic legislation on digital ID and digital wallet solutions that can enable individuals to have enhanced control over their personal data using PETs.

Conclusion

The financial services sector is reliant on cross-border data flows as financial transactions have become data transfers, market infrastructures have become data networks and financial institutions have become data processors that gather, analyze and trade customer data. The issue of cross-border data flows arising from differences in regulatory requirements is becoming ever more critical for financial inclusion, particularly with respect to cross-border payments and credit history.

The main barrier to data flows is not the lack of tools but the complexity of legal frameworks. This is true even in domestic contexts where there are several levels of government, such as in the USA, where the approach to data privacy is currently fragmented. This fragmentation poses a huge challenge for businesses with respect to cross-border data transfers. In the international context, businesses will continue to face difficulties unless data protection across jurisdictions is resolved. MSMEs are particularly impacted, as unlike larger companies they do not have the resources to navigate through different laws, definitions and sectoral regulations applying to the same sets of data.

A key issue affecting cross-border data flows today is data localization. While there are many reasons given for data localization, it all boils down to varying standards and philosophies on data protection and the lack of trust among jurisdictions in the robustness of each other's frameworks to protect citizens' data when transferred or shared across borders.

Data adequacy across economies would be the ideal solution, but it is currently difficult to achieve due to the inherent inefficiency in its application, as demonstrated by the limited number of jurisdictions that have succeeded in concluding adequacy arrangements with the EU. Without any consensus for the moment on more flexible ways to achieve data adequacy, the region will need to develop practical interim solutions that could enable firms to conduct business operations that require transferring data across borders.

While there is currently no "silver bullet" that can provide a comprehensive and definitive solution there is scope for the use of a toolbox of mechanisms to enable the expansion of cross-border data flows. These include business-level mechanisms such as contractual safeguards, binding corporate rules, certification, codes of conduct or privacy codes, statutory and administrative exemptions and wider participation in the APEC Cross-Border Privacy Rules (CBPR).

The uncertainties arising from data localization may be practically addressed through various means, such as putting rules in place requiring common and consistent standards for localization requirements as applied to different sectors; clarifying the interplay between transfer provisions in general data protection laws and localization requirements mandated by specific sectoral laws or regulations; and clarifying the scope of localization measures, the conditions under which exemptions are permitted and regulatory expectations in the implementation of localization rules for specific categories of data.

There are several initiatives that seek to improve the current situation. These include the Trans-Atlantic Data Privacy Framework, ASEAN's frameworks on digital data governance, personal data protection and data management and its model contractual clauses for cross-border data flows, and the work of the OECD, including the recent OECD Declaration on Government Access to Personal Data Held by Private Sector Entities. Private sector initiatives such as the ASEAN Banking Interoperable Data Framework (IDF) are also playing important roles in laying the foundations of the future ecosystem for cross-border data flows.

Because stakeholders come from different regions and settings, with varying levels of understanding and technical gaps, cross-border and cross-sectoral cooperation, as well as public-private dialogue are important. Policymakers need to advance the mutual recognition of core principles to protect both personal and non-personal data while ensuring cross-border opportunities. These core principles include a principles-based approach to data protection; addressing regulatory oversight concerns by rules of access instead of location; focusing operational resilience on the quality of the outsourcing solution and not its location; enhanced international cooperation; and removing barriers through international trade agreements

Privacy-enhancing technologies (PETs) have great potential as pragmatic digital solutions that can enable the processing of data in ways that comply with privacy and data protection rules is

widely recognized in key jurisdictions. They are rapidly evolving, but are at various stages of maturity, and while some are already being used widely, others are still to become operational.

Being at an early stage of development, PETs face a number of challenges. These include insufficient understanding by many regulators and consequently the lack of clear guidance that can provide certainty to businesses that the use of particular technologies are compliant with privacy requirements in their jurisdictions, which in turn hinders investment given the high cost of implementation in terms of effort, time and resources and the development of talent. Each technology has its benefits and drawbacks and degree of usefulness in bridging the privacy-utility trade-off.

APEC should play a role in this process, considering that cross-border data sharing is a key component of APEC's vision of free and open trade and investment in the region. APEC can provide a platform for (a) promoting the use of a toolbox of mechanisms to enable the expansion of cross-border data flows among member economies; (b) advancing the mutual recognition of core principles to protect both personal and non-personal data while ensuring cross-border opportunities; and (c) fostering innovation in relation to PETs by supporting research and development, secure data processing platforms, certification of trusted PETs, innovation contests, regulatory sandboxes and digital identity management.

Western Hemisphere Hybrid Roundtable

Toward Freer Safe and Trusted Flow of Data in the Asia-Pacific Region

Co-organized by
APEC Business Advisory Council (ABAC)
Asia-Pacific Financial Forum (APFF) Data Ecosystem Working Group
National Center for APEC

Venue: Institute of International Finance, Washington DC, USA

22 February 2023

AGENDA

(*Times displayed are Eastern Standard Time*)

09:00-09:10	**OPENING SESSION** **Welcome Remarks** Ms. Nicole Vukonich, on behalf of National Center for APEC (NCAPEC) **Opening Remarks** Dr. Julius Caesar Parrenas, Coordinator, Asia-Pacific Financial Forum (APFF)
09:10-10:10	**SESSION 1** **IMPLEMENTATION OF CROSS-BORDER DATA FLOWS: WHAT IS HOLDING US BACK?** Moderator: Dr. David Hardoon, CEO Aboitiz Data Innovation
	Ms. Clarisse Girot, Head, Data Governance and Privacy Unit, OECD Mr. Lee Matheson, Senior Counsel, Global Privacy, Future of Privacy Forum Mr. Duane Pozza, Wiley Law - An overview of US developments Mr. David Medine, Consultant, CGAP - Privacy in the Developing World Mr. Vinay Palathinkal, Regional Head, Wise Platform **Open Discussion**
10:10-11:10)	**SESSION 2** **POLICY AND REGULATORY INNOVATION** Moderator: Mr. Bob Trojan, CEO Token Insights and Co-Sherpa APEC Data Ecosystem Working Group
	Ms. Vivienne Artz, Co-Chair, Data Privacy Expert Group, Global Coalition to Fight Financial Crime Mr. Zee Kin Yeong, Assistant Chief Executive (Data Innovation and Protection Group) Infocomm Media Development Authority of Singapore (IMDA) Singapore

	Mr. Stephen Cheeseman, J.D., HBA, CIPP, CAMS –Head of Legal and Compliance, thinktum Mr. Gene DiMira, Advisor, Northern Block **Open Discussion**
11:10-11:25	**BREAK**
11:25-12:25	**SESSION 3** **PRIVACY ENHANCING TECHNOLOGIES: WHERE ARE WE AND WHERE ARE WE GOING?** Moderator: Mr. Bob Trojan, CEO Token Insights and Co-Sherpa APEC Data Ecosystem Working Group
	Mr. Christian Reimsbach Kounatze, Information Economist and Policy Analyst, Directorate for Science, Technology and Innovation (STI), OECD Dr. Gabriela Zanfir-Fortuna - VP for Global Privacy, Future of Privacy Forum [virtual] Ms. Caroline Louveaux, Chief Privacy Officer, Mastercard **Open Discussion**
12:25-12:30	**CLOSING SESSION** **Way Forward and Closing Remarks** Dr. Julius Caesar Parrenas, Coordinator, Asia-Pacific Financial Forum

Asian Hybrid Roundtable

Toward Freer Safe and Trusted Flow of Data in the Asia-Pacific Region

Co-organized by
APEC Business Advisory Council (ABAC)
Asia-Pacific Financial Forum (APFF) Data Ecosystem Working Group
Singapore Business Federation

Venue: Singapore Business Federation, 160 Robinson Road Singapore

25 April 2023

AGENDA

(*Times displayed are Singapore Time*)

14:00-14:10	**OPENING SESSION** **Welcome Remarks** **Mr. Jason Lee**, ABAC Singapore **Opening Remarks** **Mr. Kobsak Duangdee**, Chair, Asia-Pacific Financial Forum (APFF); and Secretary General, Thai Bankers' Association
14:10 -15:30	**SESSION 1** **Cross-Border Data Flows: Implementation and Policy/Regulatory Innovation** Moderator: **Dr. David Hardoon**, CEO Aboitiz Data Innovation
	Presentation **Mr. Mark Janson**, Partner, Digital Solutions, PwC **Panel Discussion** **Ms. Francesca Casalini**, Policy Analyst, Data governance and Privacy Unit, OECD [virtual] **Mr. Zee Kin Yeong**, Assistant Chief Executive (Data Innovation and Protection Group) Infocomm Media Development Authority of Singapore (IMDA) Singapore **Mr. Mark Janson**, Partner, Digital Solutions, PwC **Mr. Derek Ho**, Senior Vice President, Assistant General Counsel, Privacy and Data Protection, Mastercard **Open Discussion**
15:30-15:45	***Coffee Break***
15:45 -17:25	**SESSION 2** **PRIVACY ENHANCING TECHNOLOGIES** Moderator: **Ms. Irene Liu**, Managing Director, Accenture
	Presentation **Mr. Guy Sheppard**, Chief Operating Officer, Aboitiz Data Innovation

	Panel Discussion **Mr. Christian Reimsbach Kounatze**, Information Economist and Policy Analyst, Directorate for Science, Technology and Innovation (STI), OECD [virtual] **Mr. Guy Sheppard**, Chief Operating Officer, Aboitiz Data Innovation **Mr. Josh Lee**, Managing Director, Asia-Pacific, Future of Privacy Forum **Open Discussion**
17:25-17:30	**CLOSING SESSION** **Way Forward and Closing Remarks** **Dr. Julius Caesar Parrenas**, Coordinator, Asia-Pacific Financial Forum