WHITE PAPER

Proposal for TELSOM/ATRC: Advancing the ASEAN-GSMA Policy Dialogue on Cross Border Data Flows

1. Executive Summary

The purpose of this paper is to provide TELSOM/ATRC with a proposal for the ASEAN Framework on Digital Data Governance[1] (the Framework) to become operational across ASEAN, in a short time scale.

Our proposal is for policymakers to put in place a regulatory sandbox for a time bound period of 18 – 24 months[2] that would allow cross border data flows amongst the participating ASEAN countries. Whatever their level of adoption of data privacy and cybersecurity laws, Member States of ASEAN should feel able **to experiment** with cross border data flows **in a controlled environment**, for a **defined purpose** and a **predefined amount of time**.

The reason to do so is that the regulatory sandbox can be a stepping stone towards a formal mechanism for cross border data flows. These, as the World Economic Forum puts it, constitute the oxygen of a digital economy, for IoT, for start-ups, for the development of 5G.

A sandbox approach will allow the Member States also to consider and try different ways to address their legitimate cybersecurity concerns, in a way that will not delay or stop the development of a digital society, for the benefit of their citizens and SMEs. The proposed steps towards the implementation are listed in Paragraph 8 below. If we can secure the approval of TELMIN in December 2019, and if Member States can work towards the completion of bilateral or multilateral MoUs or Mutual Recognition Agreements, a sandbox could be operational early in 2020.

The GSMA would like to receive comments and refine the proposal with the ASEAN members in the period up to December 2019.

2. Introduction

In the on-going GSMA-ASEAN policy dialogue on Cross Border Data Flows, discussions with IMDA, the project lead, revealed that the TELSOM/ATRC's focus for 2019 is to implement the four initiatives of the Framework, which are:

I. ASEAN Data Classification Framework;
II. ASEAN Cross Border Data Flows Mechanism;
III. ASEAN Digital Innovation Forum; and
IV. ASEAN Data Protection and Privacy Forum framework:

---

[1] At the TELMIN meeting in December 2018 the Ministers endorsed the ASEAN Framework on Digital Data Governance. The Ministers tasked the Senior Officials to further develop and implement the initiatives under the Framework so as to enhance digital capability and cooperation among ASEAN Member States. https://asean.org/storage/2018/12/TELMIN-18-JMS_adopted.pdf

[2] The 18-24 month time frame is proposed based on GSMA research of existing regulatory sandboxes but it is not set in stone – we can discuss the appropriate length of the duration.

In recognition of the alignment of the key findings in GSMA's report on "Regional Privacy Frameworks and Cross-Border Data Flows"[3] with the Framework, it was agreed with a number of Member States in ASEAN that the GSMA should develop a proposal on the operationalisation of the Framework and present this at the TELSOM/ATRC leaders retreat in April 2019.

- In paragraph 3, we introduce the need for ASEAN to implement mechanisms to allow a gradual introduction of the safeguards needed for cross border data flows.
- In paragraph 4, we provide an overview of the participant industry and policymaker actors for the success of a sandbox, and we explain in more detail the different categories of participants.
- In paragraph 5, we list the requirements for a regulatory cross border data flow sandbox.
- In paragraph 6 we list the substantive elements of a sandbox, from eligibility criteria to risk mitigation to accountability mechanisms and evaluation criteria.
- The benefits of this are listed in paragraph 7.
- In paragraph 8 we outline the next steps; and
- in the Appendices we provide details of use cases (Annex 1) and (in Annex 2) practical mechanisms for implementation, such as MOUs.

3. A CBDF Sandbox for ASEAN

In ASEAN, the requirements around the use of personal data vary greatly from country to country. Some countries already provide a range of lawful mechanisms to transfer personal data, but some do not and others still impose localisation (or data sovereignty) measures specifically to force data to be kept in-country.

Implementing a CBDF Sandbox for ASEAN would, firstly, allow personal data to be transferred between two or more ASEAN Member States in a controlled environment that would help companies develop new products and services benefiting consumers in the region. Secondly, it would also build confidence among governments and public authorities in the region by demonstrating that it is possible to allow personal data to be transferred to another country without losing the ability to enforce domestic laws in the interests of individuals or in the interests of national security. Finally, it could also demonstrate economic advantages for ASEAN if efficiency savings, analytical insights or new business models are applied to stimulate the domestic digital economy.

A CBDF sandbox for ASEAN is not a permanent solution, but a bridging solution while ASEAN Member States develop their data privacy frameworks and develop interoperable mechanisms for cross border data flows.

GSMA's proposal is for ASEAN policymakers to put in place a CBDF regulatory sandbox open for use by mobile network operators, the IoT ecosystem, start-ups, SMEs and other stakeholders of the digital ecosystem.

GSMA would like to work with the ASEAN policymakers to use this proposal as a stepping stone towards the creation of a sandbox within the time frame outlined above and specified in Paragraph 9.

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

What is a Sandbox?

In the context of information security, a 'sandbox' refers to a segregated testing environment for new software or applications, with limited or no connection to the rest of a network, to mitigate security risks. In the same vein, a regulatory sandbox is a 'safe space' in which businesses can test innovative products, services, business models and delivery mechanisms without immediately incurring all the normal regulatory consequences of engaging in the activity in question. The concept has been mainly applied to Fintech[4], but regulatory sandboxes are emerging in regulatory areas beyond Fintech based on the demand for new products and services.

Creating regulatory sandboxes focused on protecting privacy helps companies harness increasingly available personal data to develop innovative new services, protecting consumers and adding value to them.

Examples of (national) data privacy sandboxes already exist in Singapore, through the Personal Data Protection Commission's Data Collaborative Programme[5]. In the UK the Information Commissioner is currently conducting a consultation on regulatory sandboxes.

The Global Financial Innovation Network[1] (in which Hong Kong and Singapore financial authorities participate) has announced the launch of a (cross-border) innovation sandbox for the financial services industry[6].

4. The Participants

A CBDF Sandbox for ASEAN would allow companies to demonstrate the benefits of CBDFs to consumers, companies, governments and economies by providing a controlled environment in which to test new business models; processes and products or services. For example, the ability to transfer data from different jurisdictions in a country where the data can be analysed and processed, can allow a mobile network operator to come up with new and innovative offers, to the benefit of consumers.

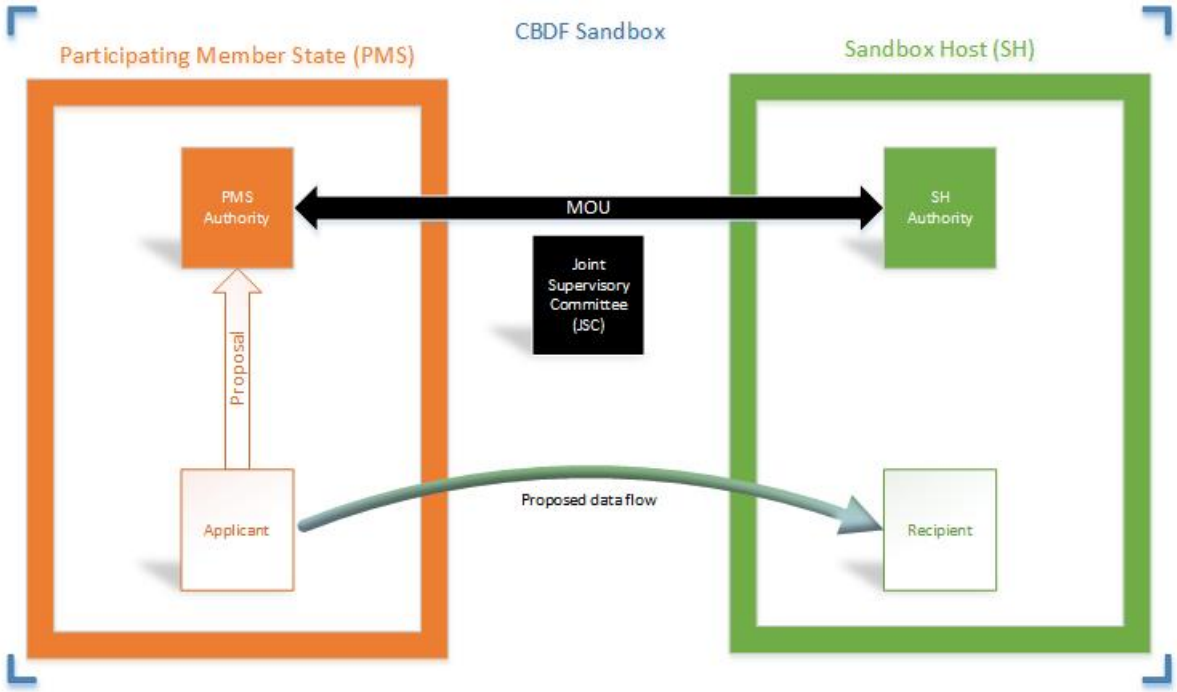
The sandbox requires the participation of at least two countries: a country which allows the data to be transferred out of its jurisdiction and a recipient country that guarantees enforcement on the home country's behalf.

The diagram and table below illustrate the key participants of the sandbox together with their roles and responsibilities.

[4] https://www.finextra.com/blogposting/15759/the-role-of-regulatory-sandboxes-in-fintech-innovation

[5] https://www.imda.gov.sg/industry-development/innovation/data-innovation

[6] https://ico.org.uk/media/about-the-ico/consultations/2260322/201811-sandbox-call-for-views-analysis.pdf



Participating Member State (PMS)
- Wishes to explore how to facilitate data flows
- Has data localisation requirements or does not have easy mechanism in place to allow data flow
- Willing to waive strict enforcement of relevant rules within the Sandbox

PMS Authority
- Has existing power to supervise data activities of Applicant
- Willing to waive strict enforcement of relevant rules within the Sandbox
- Meets the eligibility criteria set out in the Sandbox Rules
- Signs the MOU incorporationg the Sandbox Rules

Applicant
- Wishes to transfer data to recipient in third country using the Sandbox
- Must meet the eligibility criteria defined by the Sandbox
- Responsible for submitting proposal and providing sufficient information to the JSC for it to consider the proposal and supervise appropriately
- Commits to providing the data privacy safeguards set out in the Sandbox Rules to ensure that individuals' data privacy rights in the PMS are not adversely affected by the proposed movement of data
- Responsible for selecting and entering into minimum contractual obligations with the Recipient
- Commits to providing the government security and intelligence authorities with the same level of access to the in-scope data as if the data had continued to reside in the PMS except to the extent that waivers and exceptions are granted e.g: in relation to CBDF restrictions

CBDF Sandbox
- The Cross-Border Data Flows Sandbox is not physical like a server or data centre. Instead it should be seen as the entire arrangement that provides the necessary safeguards and forbearance to allow exploration of data flows in a way that protects the interests of individuals, Applicants, Authorities and Member States.

MOU (Memorandum of Understanding)
- The MOU is an agreement between two or more ASEAN Member States setting out the relevant commitments and incorporating the Sandbox Rules (see below)

Sandbox Rules

The foundational documentation that sets out:
- the purpose and scope of the CBDF Sandbox
- The eligibility requirements for each of the roles
- The minimum safeguards to be implemented and demonstrated by the Applicant

Joint Supervisory Committee (JSC)
- Under the bilateral or multilateral MOU Framework, a joint committee is established to consider proposals and supervise activities within the scope of the proposal

Proposal
- Must show evidence of meeting the eligibility criteria for proposals (e.g: tangible benefits for consumers) and how it meets the minimum safeguards Sandbox Rules accountability safeguards

Sandbox Host

Must meet eligibility criteria set out in the Sandbox Rules including that it has:
- an existing data privacy (or equivalent) law
- a functioning data privacy (or equivalent) supervisory authority that meets the criteria of the SH Authority (see below) set out in the Sandbox Rules
- a mature level of rule of law with courts and enforcement bodies that are able to take enforcement action on behalf of the PMS Authority

SH Authority
- Meets the eligibility criteria set out in the Sandbox Rules including that it is capable of taking enforcement action on behalf of the PMS Authority in relation to the Recipient or any representative or establishment of the Applicant within its jurisdiction
- Signs the MOU incorporating the Sandbox Rules

Recipient
- Must be an organisation that is able to provide a high standard of information security and meet any eligibility criteria set out in the Sandbox Rules
- Selected by Applicant in accordance with the Applicant's procurement and due diligence processes
- Must agree to the minimum contractual obligations set out in the Sandbox Rules

By definition CBDFs involve at least two countries. At a minimum, therefore, the proposed sandbox would apply to transfers of data from one Member State (the 'Participating Member State') that does not have sufficient data transfer mechanisms or that imposes data localisation requirements to a Member State (the 'Sandbox Host') that does have an

established data privacy or equivalent law with enforcement authorities that could enforce on behalf of the Participating Member State.

However, it is also conceivable that such a sandbox facility could be used by several Participating Member States and several Sandbox Host Member States. Annex 3, provides some scenarios to illustrate different possibilities.

4.1. The two main actors involved in the sandbox are therefore:

1) Industry; and
2) ASEAN Member States

4.1.1. Industry

The GSMA represents the interests of the mobile industry worldwide and also routinely considers issues in the wider ecosystem. In this capacity, the GSMA should provide the ASEAN policymakers with examples where mobile operators, regional internet companies and start-ups that have the ability to transfer data across borders can drive data innovation across ASEAN Member States and boost the growth of digital economy in the Region.

Annex 1 provides some examples of the types of products, services and business models that industry might want to test in the ASEAN CBDF sandbox.

The participants from industry will have to meet the requirements to join the sandbox, and commit to a set of binding principles and safeguards. The existing Data Protection Authorities (DPAs) in mature countries should be able to enforce the local laws against participants which may not play by the rules. As seen in the timetable in Paragraph 8 below, we propose that at the GSMA m360 Digital Societies conference in KL in September 2019, the principles of the sandbox should be explained to the industry participants and that companies be invited to register an interest ahead of what we hope will be final approval of the Ministers at the Leaders' Retreat in December 2019. After that, the sandbox can become operational.

4.1.2. ASEAN Member States

The ASEAN Framework on Digital Data Governance recognises that different levels of maturity and local laws are present in the ASEAN Member States. In practice, the creation of an ASEAN cross border data flows sandbox would require that (as a minimum) two or more Member States enter into MoUs (see Annex 2 for an MoU applied to privacy/data protection) to allow the operation of the sandbox.

Category 1: Member States with mature Data Privacy Frameworks

Malaysia, Philippines and Singapore have robust data privacy regimes that protect the privacy of citizens and have mechanisms in place to enforce privacy rules. For this reason, GSMA proposes that they should be the primary countries where a sandbox is located. Locating a sandbox in a jurisdiction where all ASEAN Member States know that there are mechanisms in place to deal with potential issues that may arise should give all the three ASEAN Member States the comfort that data can be transferred to one of these three jurisdictions.

Member States in **Category 1**, should consider how best they can ensure a form of very limited (in time and scope) mutual recognition of the respective frameworks in these countries. That is, for the duration of the sandbox, for the limited purposes for which the sandbox is set up and for the specific group of industry players eligible to use it, the three countries will consider that their respective systems are sufficient to ensure that the

purposes of a data privacy law are met. Therefore, the policymakers from these three countries should consider the sandbox as a way to test whether their systems are in fact robust enough that mutual recognition can take place generally. If so, one of the results from the sandbox approach would be to identify the criteria that national systems need to meet for mutual recognition, and another would be to lead to mutual recognition between Malaysia, the Philippines and Singapore.

Annex 2 considers the stages leading to the approval of Mutual Recognition Agreements in ASEAN, applied to privacy/data protection.

Category 2: Member States that are in the process of introducing or have just introduced Data Privacy Frameworks

Thailand's Personal Data Protection Act became law very recently. For Thailand, participation in the sandbox should mean that it gains an understanding of what is required for an appropriate operation of a data privacy regime, and can consider the results to make their forthcoming regime more robust.

Member States in **Category 2** that are in the process of introducing privacy laws or have just introduced such laws i.e. Thailand) should consider entering an MoU with the Member State(s) that are hosting the sandbox; at least until their data privacy regimes are proven to be robust.

Category 3: Member States that do not have a Data Privacy Framework

Brunei Darussalam, Cambodia and Laos as yet do not have data privacy laws; and Myanmar is at an early stage of drafting its data privacy laws. For these countries, participation in the sandbox should lead to knowledge transfers and the ability to assess in more detail the resources that they would need to introduce and implement the laws as well as the benefits to be achieved by the proper adoption of the relevant laws.

Member States in **Category 3** that do not yet have a system of privacy law may not need to do much domestically; entering into MoUs with the Member States that are hosting the sandbox and publicising the criteria for CBDFs should be sufficient.

Category 4: Member States where there are some restrictions on CBDFs

Indonesia and Vietnam have provisions (not necessarily in the privacy laws, but perhaps in cybersecurity laws or other regulatory instruments) that restrict the flow of data. For these countries, participation in the sandbox should elucidate the purpose of why it is necessary to restrict data flows and to see if there are ways to overcome the issues that would enable the law to be less restrictive without compromising the outcomes the states seek (i.e. access to data for the purpose of lawful intercept and criminal investigation).

Member States in **Category 4** may have to consider whether the operation of a sandbox for a limited purpose and a limited time could benefit from a temporary exemption/waiver from some of the provisions in existing laws.

5. The Requirements

Sandboxes have different objectives, such as attracting foreign companies with relaxed regulatory requirements[7], promoting financial inclusion[8], and advancing new technologies such as cryptocurrency[9]. Despite these different objectives, sandboxes share many common features, including:

- Eligibility criteria
  - Regulated or non-regulated organisations
- Risk mitigation: regulator waivers/letters of comfort/clearance
  - Safeguards e.g. consumers' consent, same rights, compensation
  - A formal and structured mechanism (proposal, assessment, collaboration and final report) for organisations to work with the Regulatory authority to test products, services or business models, before they are launched commercially.
- Evaluation process
  - Proposal has benefits for consumers
  - Has the business invested appropriate resources in developing the new solution, understanding the applicable regulations, and mitigating the risks
- Member States Memorandum of Understanding (MoU) and if necessary limited changes to national procedures

The tests are conducted through time-bound pilots

6. A CBDF Sandbox for ASEAN: The Substantive Elements

6.1 Eligibility Criteria

The CBDF sandbox participants will need to provide qualitative and if possible quantitative evidence that they meet the eligibility criteria. Our view is the eligibility criteria could include the following

- ***Tangible benefits***: The proposed product, service or business model should deliver better consumer choice and service innovation, economic and/or social benefits and digital capability and cooperation among ASEAN Member States.
- ***Data innovation***: The proposed product, service or business model should address a data innovation challenge that will improve product/service quality or enhance process effectiveness.
- ***Ready to test***: The participant has the appropriate resources to understand the applicable regulations and mitigate the risks, what their exit strategy will be, and how they would protect data subjects' rights.
- ***Accountability mechanism***: The participant should be able to implement binding safeguards on all entities and personnel involved and be able to demonstrate that such safeguards have been implemented and followed

[7] https://www.bankingtech.com/2018/11/arizonas-regulatory-sandbox-programme-puts-us-on-competitive-fintech-ground/

[8] https://www.unsgsa.org/files/1915/3141/8033/Sandbox.pdf

[9] https://venturebeat.com/2018/08/05/how-important-is-the-governments-new-regulatory-sandbox-for-crypto/

6.2 Regulated Industries

Requirements under current licence conditions and existing regulation that participants from regulated industries are subject to should be recognised as binding safeguards that can be taken into account to satisfy the Accountability Mechanism.

6.3 Risk mitigation for sandbox participants

The DPAs and equivalent authorities operating the sandbox may be able to provide assurances for participants that they will not take enforcement action in relation to testing activities e.g. No enforcement action letters, waivers, etc. to conduct the test within the regulatory framework.

6.4 Accountability mechanism

The participant should be able to implement binding safeguards on all entities and personnel involved and be able to demonstrate that such safeguards have been implemented and followed. Such safeguards would be similar to, but not as onerous as the EU's 'Binding Corporate Rules' or the 'APEC Cross-Border Privacy Rules'. Safeguards could include:

Binding internal procedures (or equivalent licence conditions) that ensure that:

- Appropriate notice has been given to individuals before the sandbox proposal commences to inform them about what personal data is collected, what it will be used for, how it will be used and where it will be used
- Only personal data is used that is relevant to fulfil the purposes of processing. Any data used in the pilot will be destroyed upon completion.
- Risks of harm to the individuals have been identified and either avoided or sufficiently mitigated
- The personal data used shall not be used for any purpose other than the purpose for which it was collected or compatible or related purposes
- Appropriate information security measures are in place to prevent any unauthorised disclosure
- Individuals can request a copy of personal data relating to them used in the sandbox proposal
- Individuals can easily make complaints to the participant and that such complaints are dealt with expeditiously

In addition, safeguards could include that the participant should

- impose equivalent contractual obligations on any supplier that will have access to the personal data in scope for the sandbox proposal
- make a binding declaration or commitment that individuals' rights in the home country will be respected even if the alleged infringement has taken place abroad and
- nominate a single person who is responsible for overseeing compliance with the binding safeguards within the participant and at the supplier premises

Sufficient evidence of such technical and organisational measures should be submitted during the evaluation process.

As mentioned above, there needs to be strong mechanism in place to allow DPAs or equivalent authorities to enforce on each other's behalf in order for the sandbox system to work and for participating countries to gain confidence in it.

6.5 The Evaluation Process

At the end of the period for which the sandbox is operational, it will be necessary to conduct a thorough assessment of the learnings from it, whether the objectives have been met and to determine there is scope to extend the use of sandbox to further enhance digital capability and cooperation among ASEAN Member States. Ideally the sandbox should lead to further action amongst the Member States, to allow cross border data flows under the general rules.

7 A CBDF Sandbox for ASEAN: The Benefits

Some of the key benefits of using a sandbox for ASEAN CBDF include:

- Providing industry with the option to modify their solutions before bringing them to market if they are deemed unacceptable by the regulator
- An environment for industry to deliver more efficient and cost-effective innovative services, which are compliant, socialised and acceptable to multiple stakeholders.
- Better outcomes for consumers in ASEAN as more innovative and compliant solutions are brought to market faster at potentially lower costs
- Facilitates and increases the quality of data privacy regulatory reforms that can enable innovation for ASEAN Member states by identifying regulatory barriers and developing solutions through the sandbox projects
- Encourages open, active and continuous dialogue and engagement between Regulators and industry players.
- Opportunity for ASEAN Member States and the private sectors, including SMEs, to improve digital competitiveness
- An important signal to the rest of the world that ASEAN is open to innovation
- Expanding the ASEAN Economic Community to the digital space

All proposals that are accepted into the CBDF sandbox will be required to provide quantitative and/or qualitative benefits that will be monitored during the sandbox period[10]. As can be seen from the examples in Appendix 1 beneficiaries from the sandbox are:

- ***Consumers***: Wider range of tailored solutions delivered at lower costs.
- ***Industry***: Access to ASEAN-scale digital markets.
- ***Public-sector and government*****:** Delivery of better quality public services at a lower cost and enhance digital capability and cooperation among ASEAN Member States.
- ***Society:*** Cross-border data flows across ASEAN creates new demand for ICT services, which in turn generates new businesses and creates new jobs.

8 Next Steps

- This proposal is sent to relevant policymakers within ASEAN countries, ahead of the Leaders' retreat that we understand will take place at the end of March.
- We anticipate that the policymakers will debate at this retreat a number of crucial questions such as proper oversight and enforcement and perhaps also the

[10] The more proposals that are accepted into the CBDF sandbox will lead to more robust and convincing benchmarks due to the nature of big data.

interaction between a regulatory sandbox and data classification: particularly those countries that have localisation requirements for some categories of data would wish to ensure that the sandbox allows relaxation of the rules within some parameters. In a separate exercise, the GSMA has also undertaken to consider the data classification exercise that ASEAN is also undertaking.

- To the extent that the discussions can be related back to us, we would aim to take into account the input of the Leaders' retreat's discussions before our presentation of this proposal at the **TELSOM/ATRC meeting on 8 and 9 April**. The GSMA has been invited to participate in the discussions of the Working Group and we also hope to be invited to present the proposal during the meeting of the main participants.

- The outcome of these discussions would lead to further interaction between the relevant policymakers and the GSMA to refine the proposals and create clear materials that can be shared with the industry to explain the aims and the features of the sandbox.

- To ensure industry participation, we should aim to arrange workshops in the countries in question, culminating in a presentation to the industry at m360 Digital Societies, the GSMA conference that will take place in Kuala Lumpur in September 2019. Industry should be encouraged throughout (and beyond) to register an interest with the relevant authorities.

- In parallel, the Member States should consider the ways in which they may wish to partner with other Member States, whether by way of bilateral or multilateral MOU, or by way of an MRA amongst countries with mature privacy laws.

- At the December Leaders' meeting of Ministers (TELMIN), the sandbox could be approved and become operational from Q1 2020.

Annex 1: Examples of industry proposals to test in the ASEAN CBDF sandbox[11]

Data Analytics to improve customer solutions - MNO	
Context	An MNO wants to combine copies of anonymised and aggregated customer data from its operations in two ASEAN countries and store the combined dataset in the cloud in a server located in one country.
Data Innovation	Advanced data analytics are performed across a much larger data set that enables the MNOs to provide improved offers to customers.
Ready to test	MNOs have demonstrated they have put in place the accountability mechanisms described in section 5.3.4.
Tangible Benefits	Customers in both countries benefit from more customised and innovative offers that are brought to market faster and at lower prices.
Digital transformation to streamline operations and delight customers - MNO	
Context	An MNO would like to consolidate its back office functions that are located in three ASEAN countries into a single virtualised group-wide data centre.
Data Innovation	Using advanced technologies, such as machine learning, to simplify and digitise back office functions.
Ready to test	MNOs have demonstrated they have put in place the accountability mechanisms described in section 5.3.4.
Tangible Benefits	Customers received improved quality of service as the MNO was able to reduce the number of support calls by anticipating the problems. Improved efficiency for the MNO by spreading its capital and staffing costs across all customers in their footprint
Internet of Things (IoT) tracking solution – Regional Telco	
Context	A Regional Telco would like to launch an IoT solution across ASEAN that allows consumers to locate, monitor and track valuable assets and inventory that are critical to their business operations.
Data Innovation	A new IoT edge and device management solution was developed to track the assets. A machine-learning model that has records of the customers fleet management assets and receives new data in real time to predict if the assets are at risk of being lost/stolen.
Ready to test	The Regional Telco has put in place the accountability mechanisms described in section 5.3.4
Tangible Benefits	Customers are able to remotely track their assets and reduce risk to their business, save money, and create new revenue streams.

[11] Examples adapted from industry use cases. This list should not be seen as exhaustive and facts and findings are applicable to all new services which exist (but are not listed here) or will come to the market with 5G and/or ultrafast broadband services.

Annex 2: Mutual Recognition Agreement and Memorandum of Understandings applied to privacy/data protection

Mutual Recognition Agreements (MRA) are one of the instruments utilised by ASEAN to remove non-tariff trade barriers and facilitate the free flow of goods in the region in order to realise the establishment of the ASEAN Economic Community. [12]

MRAs are agreements between Member States that provide for mutual recognition of the results of conformity assessments conducted in one Member State by authorities in the other ASEAN Member States. MRAs typically provide an exporting party with the authority to test, inspect and/or certify products, against the regulatory requirements of the **importing** party, **in its own territory and prior to export.**

This basic MRA framework can be applied to data protection/privacy requirements across ASEAN Member States to facilitate the free flow of data across the region. We propose that Category 1 countries (i.e. Malaysia, the Philippines and Singapore) enter into an MRA with **mutual recognition obligations** for data transfers, based on the robust privacy requirements in each country.

Example of MRA stages in ASEAN, applied to privacy/data protection:

Stage	**Description of Process in ASEAN MRA Guidelines**	**Suggested implementation for data flows**
Preliminary Proposal for an MRA	The proposal may be initiated by any Member State or by the ASEAN Secretariat. Agreement to proceed would be by consensus of the concerned Working Group (WG).	This process would be the same or similar, with decisions made by the TELSOM/ATRC
Impact Assessment	The WG concerned would decide on the scope and method for conducting the assessment. Funding for the assessment will be identified and implementation coordinated by the WG responsible with the support of the ASEAN Secretariat.	The impact assessment process is designed to "identify benefits, compare alternative approaches and identifying risks" (per the MRA Guidelines). This sandbox proposal sets forth information necessary to conduct this impact assessment (see benefits identified in section 8 of the proposal)
Confirmation of Scope and Objectives	The WG concerned will review the results of the impact assessment and decide on the proceeding and on a positive decision; the WG will decide on the scope and objectives of the proposed MRA.	Suggested scope and objectives are noted in this proposal.

12 https://www.asean.org/storage/images/Community/AEC/Sectoral/standarandconformance/Guidelines%20for%20The%20Development%20of%20Mutual%20Recognition%20Arrangements-rev3-FA.pdf

Preparation of Working Draft of the MRA	A working draft will be prepared. The WG may request a Member State, the ASEAN Secretariat or any external party for this.	The same process could apply. In terms of content of the draft (based on obligations in existing ASEAN MRAs[13]): • Elements of the existing ASEAN Privacy Framework could be used as a foundation/starting point for identification of mutual recognition obligations; • Transparency obligations (e.g., identifying a contact point in each Member State involved) would be included; • Each Member State involved would be required to identify a Competent Authority and notify the Secretariat accordingly. The Competent Authority would be authorised through the MRA to enforce the MRA requirements. • The MRA could also include requirements around provision of technical assistance to other Member States involved in the MRA.
Deliberation of the Working Draft by WG Members Leading to the Development of a Draft for Member States' Consultation	The "draft for consultation" is a preliminary draft and does not bind Member States. It should reflect the general principles and may include alternative texts for sections in which there is no agreement. It is a document to facilitate Member States to conduct consultation with stakeholders in each Member State.	This process could be the same
Consultation with Stakeholders within Each Member State	The consultation process is undertaken independently by each Member State. Each Member State will use the results of the consultation to formulate its position in preparation for deliberations of the MRA with other Member States.	This process could be the same
Development of a Final WG Draft	The WG concerned will reconvene deliberations, taking note of the results of consultations. The negotiations	This process could be the same, albeit with the MRA approved by the TELSOM ATRC

[13] http://agreement.asean.org/media/download/20180522045752.pdf

	will continue till the objective of Member States reaching agreement on the content of the MRA is achieved. On completion, the draft MRA is submitted to the ASEAN Consultative Committee on Standards & Quality (ACCSQ) or other body responsible for the WG as appropriate.	
Finalisation	The finalisation will include legal vetting and approval by the appropriate ASEAN body. This will be coordinated by ASEAN Secretariat. The WG responsible will be informed of progress.	See above

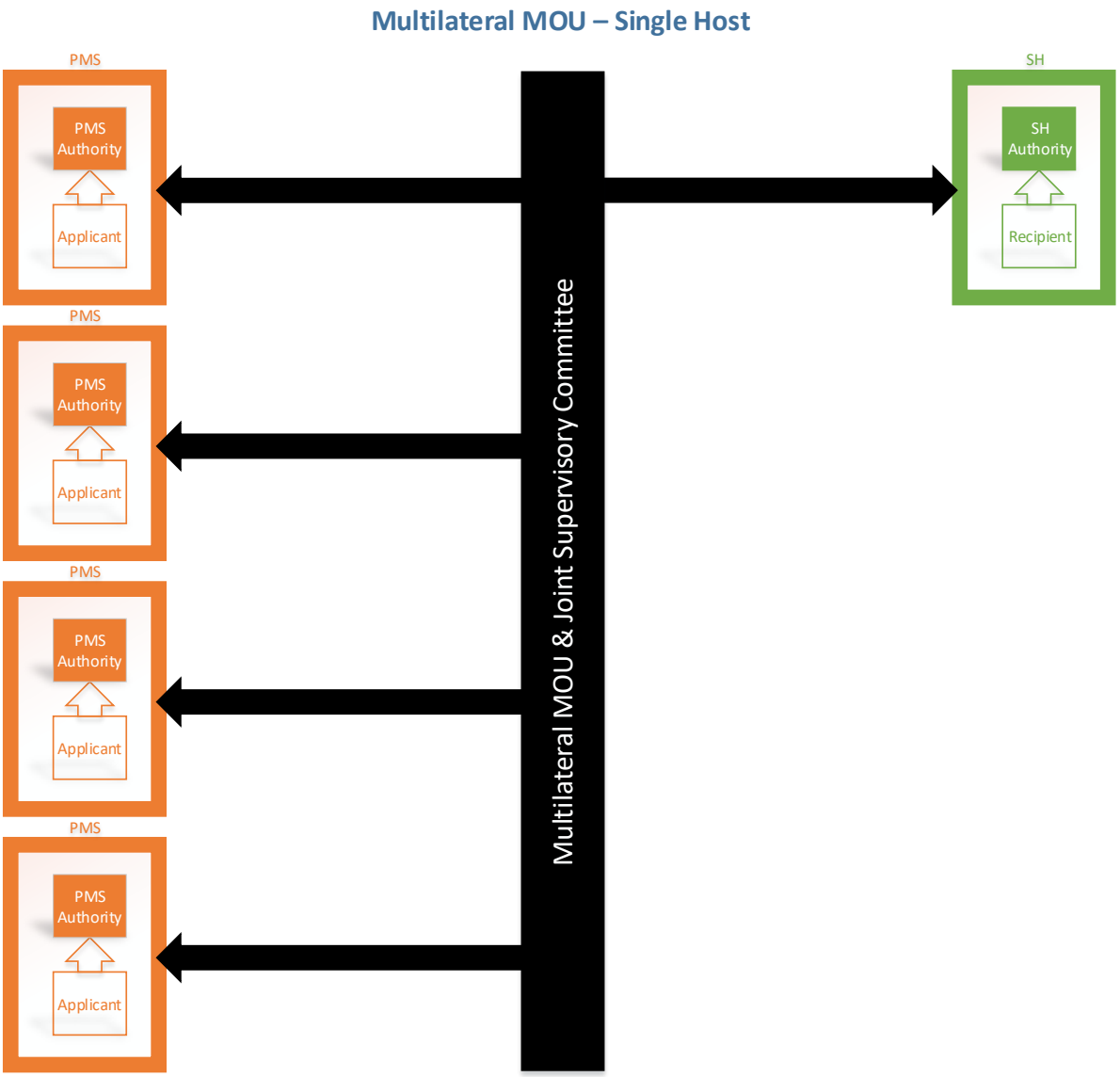
Memorandum of Understandings (MoUs)

Alternatively, given the robust nature of their existing privacy frameworks, these countries could enter into bilateral MoUs or a tripartite MoU focused on ensuring the cooperation of the relevant regulatory authorities (e.g., sharing enforcement data and cooperating on enforcement). The MoU between the U.S. Federal Trade Commission and the Data Protection Authority of the Netherlands is an example of such an agreement.[14]

The MoU applies to mutual assistance and the exchange of information for the purpose of investigating, enforcing and/or securing compliance with Covered Privacy Violations, defined as "practices that would violate the Applicable Privacy Laws of one Participant's country and that are the same or substantially similar to practices prohibited by any provision of the Applicable Privacy Laws of the other Participant's country." This MoU includes obligations similar to those contained in an MRA, such as specific elements of cooperation and technical assistance. However the MoU does not specify the practices that would violate applicable privacy laws in each country.

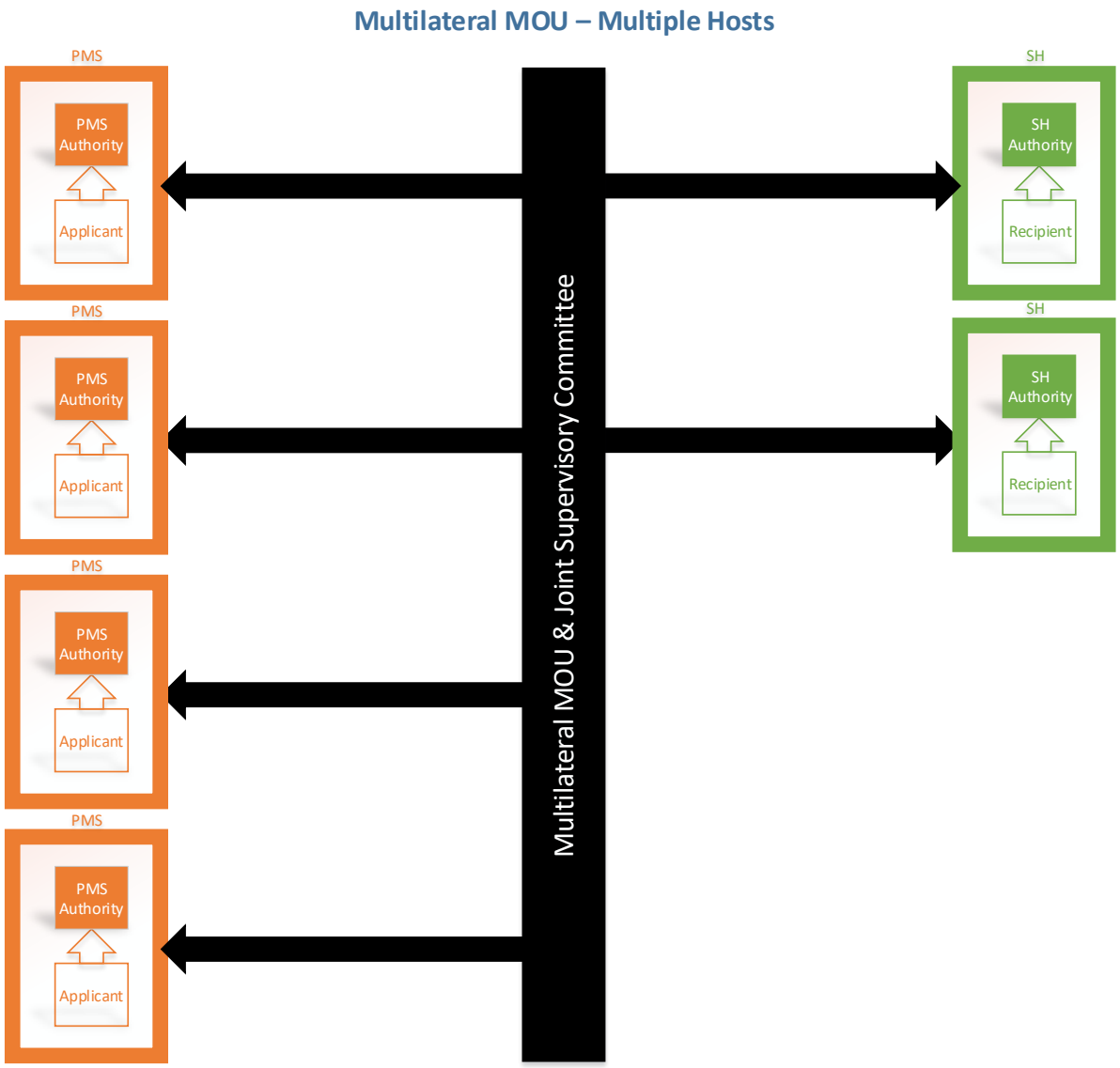
[14] https://www.ftc.gov/system/files/documents/cooperation_agreements/150309ftcdutchcb-1.pdf.

Annex 3: Sandbox Scenarios for ASEAN Member States and sandbox hosts

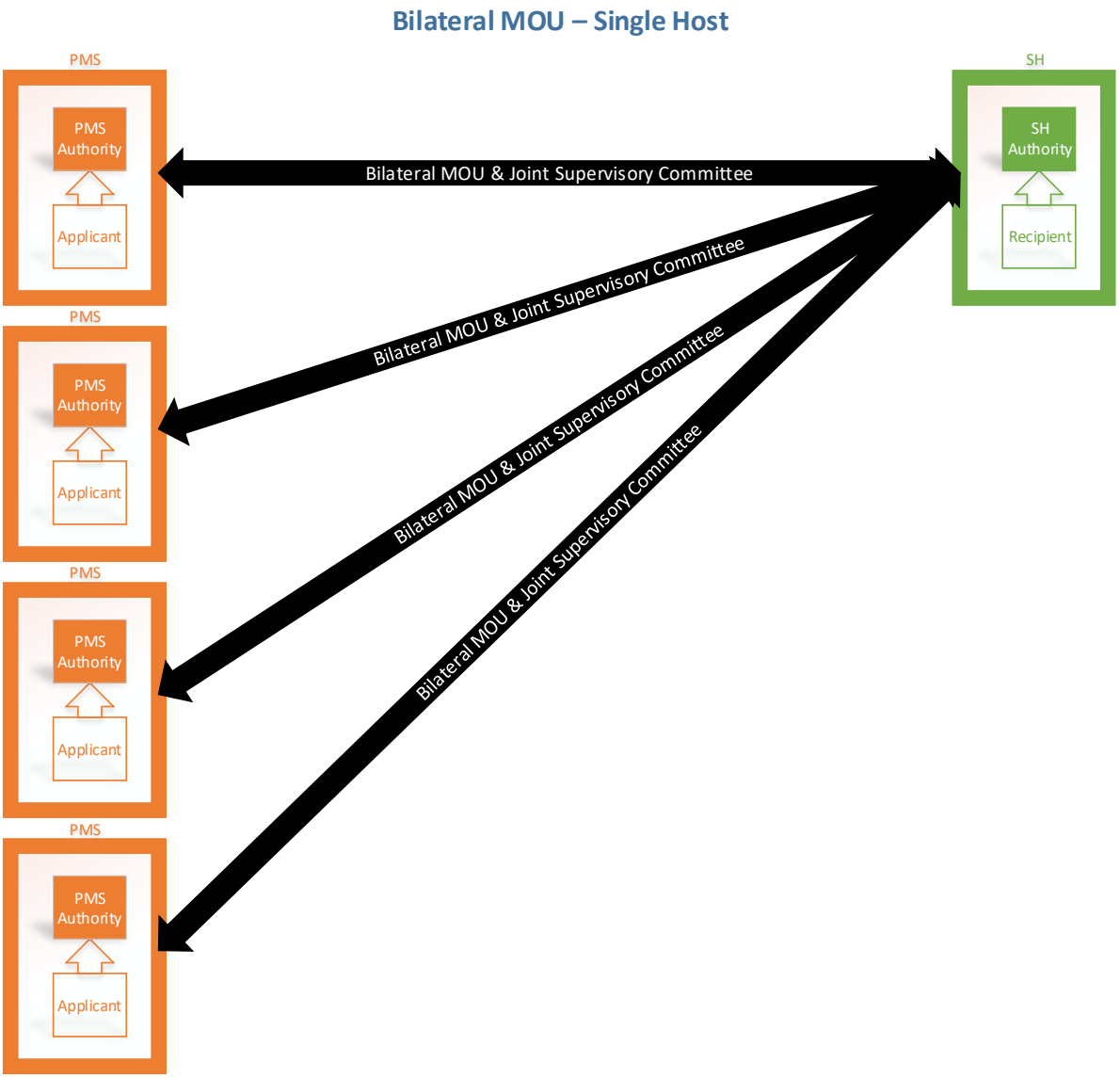


PMS= Participant Member State SH = Sandbox Host

Annex 3: Sandbox Scenarios for ASEAN Member States and sandbox hosts



Annex 3: Sandbox Scenarios for ASEAN Member States and sandbox hosts



Annex 3: Sandbox Scenarios for ASEAN Member States and sandbox hosts