# ROUNDTABLE ON
# BIOMETRIC DATA SHARING FOR IDENTITY VERIFICATION
## Introduction to the Regional Data Sharing Initiative

**Overview**

The Asia-Pacific region is characterised by dynamic and diverse forms of migration. Criminal networks actively seek to exploit weaknesses in immigration borders and have become highly sophisticated in their ability to quickly change their modus operandi to counter disruption efforts by governments.

Regional cooperation has become increasingly important to manage the movement of people across borders, particularly to effectively combat transnationally operating criminal networks, protect vulnerable populations and address the challenges posed by those exploiting the gaps in border security, and states intelligence systems. Since the launch of the Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime in 2002, member states have sought to develop more harmonized responses to people smuggling, trafficking in persons and related transnational crime through regional cooperation and in line with international standards. The issues of irregular migration, border control and identification of irregular migrants have been at the center of a number of Bali Process meetings over the past years.

There is a growing demand among Bali Process Member States for programs to help build national and regional capacities in areas such as the establishment of traveler's identity, early detection of fraudulent documents and criminal activities, information sharing of the immigration data, understanding of international obligations under international law, capacity to identify persons in need of international protection and vulnerable migrants.

At the 5th meeting of the Bali Process Ad Hoc Group Senior Officials, participants agreed to take forward recommendation to develop practical measures to implement the RCF in line with the Bali Process Steering Group Note on *Operationalisation of the Regional Cooperation Framework in the Asia Pacific Region*. This included developing best practice models on refugee protection and international migration including reception, registration and biometric collection, irregular migration, and migration management including border management as they relate to the Asia-Pacific region.

At the 8th meeting of Bali Process Ad Hoc Group Senior Officials, participants endorsed the Bali Process Strategy for Cooperation: 2014 and Beyond, in which members directed the Regional Support Office to the Bali process (RSO) to explore opportunities to expand the outcomes of existing bilateral and multilateral biometric data sharing arrangements.

In the line with the above, the RSO is exploring opportunities to expand the outcomes of existing bilateral and multilateral biometric data-sharing arrangements to strengthen regional border management capabilities by addressing key issues that correspond to the collection and sharing of biometric data. To further this work, the RSO proposes to implement the Regional Data Sharing Initiative (RDSI) with the aim of developing a technological solution that facilitates biometrics data

sharing among participating member states and a policy framework to support operation of a technological solution that considers legal and policy considerations, and biometric standards and capabilities.

**Purpose**

The RDSI project aims to facilitate biometric data sharing between participating Bali Process members in order to contribute to the early detection of smuggling and trafficking of people, and provide evidence for the investigation and prosecution of these crimes. In line with national privacy laws and international obligations, the project has the potential to allow for efficient and quick identification and information exchange for processing refugee and asylum seeker claims and assist in identifying vulnerable migrants.

The project aims to encourage regional cooperation to reduce irregular people movement by enabling members to share biometric by aligning legal, technical, privacy and business processes to domestic and international frameworks.

The project will deliver technical capability and encourage regional cooperation for the sharing of biometric data in relation to people movement across and within regional countries' borders, to enable more effective cooperation both between countries, and between countries and international organisations.

**Objectives**

The key objectives of the RDSI project are:

- to develop comprehensive understanding of the privacy implications and legislative requirements for the sharing of data between Bali Process member states and participating organizations;
- to create more effective multilateral information and intelligence sharing system consistent with diverse national privacy laws and international legal obligations;
- to develop a framework to facilitate data sharing between participating countries and organizations;
- to implement a technical solution through which Bali Process member states and participating organizations can share data for the purpose of identity verification;
- to enhance Bali Process member states' capacity to effectively respond to crimes of human trafficking and people smuggling in the region, and to provide protection for those in need;
- to promote cooperation between Bali Process member states and participating organizations in sharing biometric and other data; and
- to advance the implementation of an inclusive non-binding regional cooperation framework under which interested parties can cooperate more effectively to reduce irregular movement through the region.

**RDSI framework and activities**

The project composes of two main elements:

- the development of a technological capability (the Technical Solution) for sharing of biometric data, envisioned to be a model in which members share biometric data directly with each other through a secure server; and
- the development of a policy framework (the Framework) to govern the use of the Technical Solution. The recommended Framework should consider including an overarching Terms of Use and associated bilateral arrangements that would support the operation of the Technical Solution in accordance with domestic laws and applicable international standards.

This is to be achieved through a consultative process supported by the RSO. The consultative process will involve identifying the challenges and solutions on how biometric data for identity verification can be shared amongst Bali Process members during a consultative Roundtable on Biometric Data Sharing for Identity Verification. It is envisaged that biometric policy, legislation, privacy and data protection; biometric standards and capabilities; technical challenges to adopting biometric systems; and data sharing arrangements between Bali Process members will be discussed. This activity will aim for the participants to develop recommendations and consider next steps for progressing regional biometric data sharing initiatives.

Following the Roundtable, a Biometric Data Sharing Review Committee (the Committee) is to be established to oversee the development of a Framework and Technical Solution. The outcomes will be presented for endorsement at the 6th Ministerial Meeting in 2015. The Committee will operate in accordance with the draft terms of reference (TORs) developed by the RSO. The Committee is expected to meet at least twice during the life of the project.

The content of the Technical Solution and the Framework will be decided through consultative processes with Bali Process members and through the Committee. The drafting will take into account the policy and legal considerations such as effectiveness, cost, feasibility, legal authority of government agencies, human rights and other protections, privacy and data protections, and framework administration. As part of the consultative process, members will be given the opportunity to test the Technical Solution and to provide comments and feedback**.**

Upon successful completion of consultation process, the Framework and Technical Solution will be presented to a Bali Process Ad Hoc Working Group at a consultation workshop and, once endorsed, presented to the Ministers at the 6th Ministerial Meeting.

**ROUNDTABLE ON**
**BIOMETRIC DATA SHARING FOR IDENTITY VERIFICATION**

## Discussion paper: Possible Framework for Regional Data Sharing Initiative

### Executive Summary

The Regional Support Office to the Bali Process (RSO) is developing a Regional Data Sharing Initiative (the RDSI) that aims to provide a comprehensive solution to facilitate harmonized, effective and timely biometric data sharing among participating members, consistent with member state's national legislations and international standards.

The global practice of sharing of biometrics data is increasingly proving to be an efficient and effective method for verifying identity of migrants and a way of recording migration flows between borders. Bali Process member states use biometrics recognition systems for travel, immigration, and national identification purposes. While biometrics technology is being adopted among Bali Process members, effective mechanisms to share biometric data regionally in a simple and secure manner to address irregular migration, people smuggling and human trafficking are yet to be developed.

Building on the strong interest in biometric systems and technology expressed by Bali Process during the fifth and eighth meetings of the Bali Process Ad Hoc Group Senior Officials this paper presents an option a policy framework (the Framework) to operationalize a data sharing technological solution (the Technical Solution) that is to be discussed at the *Roundtable on Biometric data sharing for identity verification* to be held on 15 and 16 October 2014 in Bangkok.

While the Technical Solution is aimed to be a simple channel of communication of biometric data, many technical, legal, policy and administrative issues need to be considered. These issues include developing a Framework that addresses complex legal and policy contexts that include international human rights obligations, diverse domestic legal systems, and international, regional and domestic privacy frameworks. These issues are discussed in separate sections of this paper.

**Section one** explains the concept and use of biometric data within the Bali Process context and discusses the biometric data sharing context that would apply to Bali Process members.

**Section two** summarizes different framework options available to implement the RDSI. Noting the voluntary and non-binding nature of the Bali Process, a framework is recommended based on an analysis of numerous legal and policy considerations which are explored in detail in the 'Policy and legal risk and mitigation' table provided at Attachment A. The recommended framework consists of an overarching principles or "Terms of Use" that sets out the minimum standards and safeguards for participation in the Framework. The Terms of Use will be adopted by a network of secondary agreements between participating members that contain specific details of data sharing arrangements as well as any potential safeguards additional to the minimum safeguards set out in the Terms of Use. An initial draft of the Term of Use is included at Attachment B.

The recommended framework would offer the following benefits:

- a harmonized and consistent approach to biometric data sharing between member states;

- flexibility and dynamism to accommodate the specific bilateral relationships and diverse domestic contexts of member states. For example, depending upon the relationship between the parties, bilateral arrangements may be binding or non-binding;
- any endorsed Terms of Use would contain minimum standards and safeguards that are specific to this framework only and would not act, or be seen, as a general declaration of principles that applies to anything outside the framework; and
- reduction in duplication of agreements and negotiation time for bilateral negotiations if rules and minimum standards and safeguards have already been agreed.

**Section three** proposes possible administrative arrangements for the Framework, including arrangements for a committee supported by the RSO to be the primary body responsible for administrative and oversight purposes.

**Section four** provides an overview of the possible features of the proposed Technical Solution, taking into account the policy considerations set out in the 'Policy and legal risk and mitigation' table provided at Attachment A.

# Section One: Use of biometric data

Biometrics (or biometric recognition) is defined by the International Standardisation Organisation as the "automated recognition of individuals based on their biological and behavioral characteristics". The biological and behavioral characteristics are those from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition."[1] Biometric data can include fingerprint recognition, face recognition, DNA matching, eye (iris and/or retina) recognition, and signature recognition. Based on current adopted technologies by both government and private entities, fingerprint and facial images are the most widely used form of biometric data.

For many Bali Process member states, biometrics are being used, or proposed to be used, for travel, immigration, nationality and national identification purposes (either in passports and national ID cards or both). In some countries, biometrics are also used for identification for social security, criminal investigation and disaster relief purposes.

Biometric data is increasingly seen as an advanced method of effective and efficient identification of individuals. In particular, sharing biometric data between countries utilizes the greater database resources of partnering countries and can provide a more timely and effective mechanism to identify individuals whose identity are unknown or uncertain, and to combat identity fraud.

Within the Bali Process context, potential uses of biometrics for identification purposes include:

- Checking of visa applicants, displaced persons, asylum seekers, residency applicants, transit passengers to determine whether they are:
    - known or suspected terrorists (including foreign fighters)
    - victims of human trafficking
    - engaged in serious criminal activity or
    - involved in funding/collecting donations for prescribed organizations
- Checking of visa applicants and persons seeking protection to determine whether they are making asylum claims in multiple jurisdictions and are "forum shopping"
- Checking of visa applicants to determine whether known or suspected sex tourists/sex offenders
- Detecting persons (asylum seekers or displaced persons) who have already received protection from a 3rd country (country of first asylum) or have been registered as a refugee by the UNHCR
- Ability to re-document genuine visa or passport holders who have had their travel document lost/stolen/withheld
- Checking of travel documents against white lists and black lists held in country or organization of issue

### Biometric data sharing within the Bali Process context

Due to the large membership of the Bali Process, any inclusive framework for regional biometric data sharing must balance the desire for a harmonized and consistent approach with the diverse and complex domestic contexts of member states. The domestic contexts of member states may have

[1] ISO/IEC 2382-37. Information Technology – Vocabulary – Part 37: Biometrics

key variables that result in different approaches and policy considerations when sharing biometric data. For example, member states would have varying uses and capabilities for biometric data for identification purposes. Different immigration and law enforcement agencies may also have different legal authorities to collect, use and disclose biometrics and other immigration related information.

There are also key legal variables. For example, the privacy and data protection systems of member states, including avenues for access and correction of personal information held by government agencies, vary greatly. These privacy and data protection systems may also operate within different regional and international privacy principle frameworks such as the UN Guidelines for the Regulation of Computerized Personal Data Files, EU Data Privacy Directive, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the APEC Privacy Framework.

Member states may also have varying international obligations including the non-refoulement principle and the Universal Declaration of Human Rights, and where applicable, the Refugees Convention, the International Convention on Civil and Political Rights, the Convention Against Torture, the Convention on the Rights of the Child, and the UN Convention on Transnational Organized Crime.

In addition to balancing these key variables, any framework must also operate alongside existing data sharing and biometric sharing mechanisms between members. Such arrangements include formal multilateral mechanisms such as Eurodac, Five Country Conference (FCC), Interpol's i24/7 communication system and Automated Fingerprint Identification System (AFIS), Agreement on Information Exchange and Establishment of Communication between some ASEAN countries, UNODC Voluntary Reporting System – Migrant Smuggling and Related Crime (VRS-MSRC) as well as informal and ad-hoc arrangements between countries.

The proposed framework should be developed to incorporate several features that will complement and not overlap with these pre-existing arrangements.

The Framework is intended to apply to a greater number of countries in the region than FCC or Eurodac. The Bali Process encompasses 45 member states and 3 member organizations in the region, significantly more than the FCC member countries or the Eurodac network, which can only potentially be used by New Caledonia.

Unlike Interpol or Eurodac, the proposed Framework should not host a central database that stores biometric data and other personal information. This reduces privacy risks as well as enabling countries to share data bilaterally without concerns of building a central database.

The use of the Framework may be broader than the crime and law enforcement uses of the Interpol databases. While there may be a broad overlap between the uses of both mechanisms, the Framework may additionally be used for identity verification for migration, refugee and resettlement purposes.

Since the Framework is intended to be used simply as a channel of communication that may facilitate or initiate further information sharing and cooperation, it should complement and not overlap or conflict with general criminal information sharing frameworks. For example, countries may prefer to use the Framework as a preliminary investigative tool, and where a match exists, use

more complex systems like through Interpol or the Mutual Legal Assistance framework to request further assistance.

Since the Framework only shares biometric data for identity verification, it will be used for specific identification and operational purposes, rather than more general non-nominal trends based information sharing such as through the VRS-MRSC.

Unlike any informal ad-hoc arrangements in existence, the Framework will offer countries an option to implement a more formalized, transparent and consistent arrangement.

Finally, as a voluntary framework, countries can opt in and opt out of the Framework, and choose whether or not to use it in any particular circumstance.

# Section Two: Framework options and recommendations

## Policy and legal considerations

In developing any framework, policy and legal considerations and risks need to be assessed and mechanisms need to be established to mitigate these risks. These policy considerations and risks include ensuring the effectiveness of biometric data sharing to address irregular migration, people smuggling and human trafficking purposes, and the effectiveness of sharing between different systems and standards of member states.

Other policy considerations and risks include whether government agencies have lawful authority to collect and share biometric data, privacy and data protection, and international legal obligations including human rights and refugee protection. A table outlining these policy and legal considerations, and the mitigation options available, is available at Attachment A.

## Framework options

The following is a summary of the key benefits and challenges of various framework options.

| | |
|---|---|
| A legally-binding multilateral agreement, most likely a treaty, which provides for all the procedural and legal obligations. This would be similar to the Eurodac system which is regulated by the binding Eurodac Directive. | Benefits:<br>· A legally binding agreement ensures certainty, enforceability and maximum protection and safeguards<br>· A multilateral agreement creates consistency<br><br>Challenges:<br>· Multilateral negotiations requiring agreement between many participants may be lengthy<br>· Difficulties in addressing the needs of diverse legal and policy contexts within one agreement<br>· Many member states may not be willing to enter into a legally binding agreement |
| Non-binding multilateral agreement, such as a Memorandum of Understanding (MOU). This would be similar to the Agreement on Information Exchange and Establishment of Communication. | Benefits:<br>· A non-binding agreement means more member states may be willing to participate<br>· A multilateral agreement creates consistency<br><br>Challenges:<br>· A non-binding agreement means less certainty, enforceability and protections and safeguards<br>· Multilateral negotiations requiring agreement between many participants may be lengthy<br>· Difficulties in addressing the needs of diverse legal and policy contexts within one agreement |
| A network of binding bilateral agreements. This would be similar to the Mutual Legal Assistance Treaty framework. | Benefits:<br>· A legally binding agreement ensures certainty, enforceability and maximum protection and safeguards<br>· Bilateral agreements based on model agreements create some consistency while also providing flexibility to meet the needs of diverse bilateral relationships<br><br>Challenges:<br>· Complex system of bilateral agreements may result in |

| | |
|---|---|
| | too little consistency for one Technical Solution.<br>· System of bilateral agreements alone may create duplication of effort for members during negotiation and administration of the agreement and use of the Technical Solution<br>· Some members may not be willing to enter into a legally binding agreement |
| A network of non-binding bilateral agreements. This already exists through informal or ad-hoc arrangements between members. | Benefits:<br>· Non-binding agreements may mean member states are more willing to participate<br>· Bilateral agreements based on model agreements create some consistency while also providing flexibility to meet the needs of diverse bilateral relationships<br><br>Challenges:<br>· A non-binding agreement means less certainty, enforceability and protections and safeguards<br>· Complex system of bilateral agreements may result in too little consistency for one Technical Solution.<br>· System of bilateral agreements alone may create duplication for members during negotiation, administration and use of the Technical Solution.<br>· Informal and ad-hoc arrangements provide less formality and transparency. |

**Recommended Framework**

As seen from the table above, each option has its own benefits and challenges, however given the diverse technical, legal and policy contexts of member states, the solution should contain a bilateral element to ensure enough flexibility to accommodate the specific dynamics of each bilateral relationship.

The preferable and desirable elements of a Framework are:

- Non-binding arrangements to reflect the non-binding nature of the Bali Process and facilitate greater agreement and participation
- Multilateral elements to create harmony and consistency
- Multilateral elements to reduce duplication for member states during negotiation, administration and use of the Technical Solution
- Bilateral elements to provide flexibility to meet the needs of diverse bilateral relationships

The recommended Framework incorporates a combination of the features of the above framework options. One example of such a combination is the arrangements under the FCC. Under the FCC, an umbrella High Value Data Sharing Protocol establishes a consistent overarching framework in which data is shared through one technical solution, the Secure File Sharing System. Supplementing this overarching framework is a network of secondary agreements between each of the five countries that addresses the specific dynamics of each bilateral relationship.

Similarly, within the non-binding, diverse context of the Bali Process, a Framework could contain:

- an overarching set of rules known as the "Terms of Use" endorsed by the Bali Process membership that sets out the rules and minimum standards and safeguards for participation in the Framework (an early draft example of this document can be found at **Attachment B**); and
- a network of secondary bilateral agreements between participating members that adopt the Terms of Use and add any specific details or additional safeguards relevant for each participating member, taking into account the diverse dynamics of each bilateral relationship.

Through the Terms of Use, a harmonized and consistent approach to biometric data sharing can be maintained between member states. A Terms of Use setting out rules and minimum standards and safeguards will also reduce duplication, time and effort when negotiating secondary bilateral agreements. Further, any endorsed Terms of Use would contain minimum standards and safeguards that are specific to this framework only and would not act as, or be seen as, a general declaration of principles that applies to anything outside the framework.

Through a network of secondary bilateral agreements, flexibility and dynamism is created to accommodate the specific bilateral relationships and diverse domestic contexts of member states. For example, depending upon the relationship between the parties, bilateral arrangements may be binding or non-binding.

## Section Three: Framework administration

Any administration of the Framework should ensure that the legal and policy risks continue to be assessed and mitigated throughout the lifetime of the Framework. The Framework should be administered by the RSO as a centralized and independent focal point. Consistent with Bali Process practice, a committee established by Senior Officials of the Bali Process Ad Hoc Group, consisting of no less than five Ad Hoc Group members and supported by the RSO, should be the primary body responsible for administrative and oversight purposes.

Administration mechanisms can include:

- Periodic and confidential reporting on transactions to build confidence in the Framework and to ensure that data sharing is low volume.
- Questionnaires and requests for case studies to understand uses of the system and ensure that data sharing is high value.
- Suspension or cancelling participation if there is any use of the Technical Solution inconsistent with the Framework.
- Open dialogue to allow technical refinements to the Technical Solution as necessary.
- Open dialogue to allow for any complaints and concerns to be raised.

## Section Four: Possible features of the Technical Solution

The following are possible features that could be incorporated into the Technical Solution, taking into account the legal and policy considerations and Framework features discussed in this paper:

- Mechanisms to ensure that requests remain low volume
- A Request tool that, prior to sending the request, seeks specific information relating to
    - Biometric data to be matched (fingerprint, photograph)
    - The countries from which matches are requested
    - Purpose of the request (for irregular migration, people smuggling, trafficking or other related transnational crime)
    - Whether a person has made a claim of persecution, and if so, against which country.
    - Whether a person has made a claim of torture, or cruel, inhumane or degrading treatment, and if so, against which country.
- A Response tool that only provides "match" or "no match" response.
- Technical business rules that incorporate any minimum standards and safeguards, or additional safeguards. For example, if a user enters information that a person has made a claim of persecution against Country A, the Technical Solution will not allow requests to be sent to Country A.
- Mechanisms to ensure that data retention within the Technical Solution is limited, with all data sent through the system deleted after the request/response has been completed, or automatically deleted after a set maximum period (for example, 5 days).
- No biometric data should be retained, and only transactional data will be retained for administrative purposes.

The specific features of the Technical Solution will be determined through the consultation with interested member states, outcomes of meetings and workshops through the Bali Process and any relevant Bali Process working group or committee.

## Attachment A: Policy and legal risks and mitigation

| Policy consideration or risk | Mitigation options |
|---|---|
| The Framework must be effective in addressing irregular migration, people smuggling, trafficking in persons and related transnational crime. Given the ongoing development of members' technological capacity, data sharing should not unduly burden members' resources and systems. | Data sharing is proposed to be:<br>• "low volume" to ensure that sharing remain within the technical capacity of members' systems; and<br>• "high value" to ensure that the low volume of data shared has maximum effect.<br><br>Bilateral arrangements can allow members to flexibly determine the data sharing arrangements that is most effective for them. |
| Data sharing is effective only if the biometric data can be shared and understood by different countries and systems. | Standard formats (such as the NIST format for fingerprints) should be used wherever possible.<br><br>The Technical Solution should also be capable of interpreting different information, standards and formats and re-configuring them for different participating members. |
| Any framework must complement and not unduly overlap or conflict with existing data sharing mechanisms. Otherwise, any inconsistencies and overlapping between the frameworks will undermine the effectiveness of both mechanisms. | The Technical Solution should act as a simple channel of communication to establish whether there are any biometric matches between participating members. The Technical Solution should be used as a starting point for further data sharing, which may take place through other arrangements.<br><br>The framework should provide that the Technical Solution does not prejudice any other data sharing mechanism and should be used to complement and support those other mechanisms. |
| The proposed framework will only be effective if it can be used within the diverse legal and policy situations of member states.<br><br>Due to the diversity of these situations, a uniform set of rules for the Framework may act to exclude some countries, either because they cannot meet the minimum standards of the Framework or because their legal and policy requirements will not allow them to participate in such a system. | The Framework should remain flexible and dynamic wherever possible. While minimum standards and safeguards should be created, it must be acceptable to all member states. Flexibility and dynamism can be achieved through countries negotiating their own individual bilateral or multilateral agreements and business rules for data sharing through the Technical Solution.<br><br>Any individual agreement may provide additional safeguards, but must not be inconsistent with the minimum standards and safeguards set out in the Terms of Use. Any individual agreement must state that the minimum standards and safeguards will prevail to the extent of any inconsistency. |
| The effectiveness of the Framework, and any trust or confidence developed, will be seriously undermined if the | The Terms of Use should provide the following minimum safeguards:<br>• The Technical Solution should only be used for the |

| | |
|---|---|
| Framework is misused for improper purposes.<br><br>There may also be concerns that, over time, there is a "purpose creep" where the Technical Solution is used beyond the original scope envisioned. | purpose of identity verification for irregular migration, people smuggling and trafficking in persons purposes. Non-compliance may result in the country being removed as a participant.<br><br>• Amendments to the scope and purpose of the Framework need to be endorsed by the whole Bali Process membership. |
| While the Bali Process is an inclusive, non-binding process, the sharing of personal information (in the form of biometrics) means that there should be a level of enforceability of any rules to mitigate the risk of improper use or privacy breaches. | Member states will be well aware of the importance to build trust and confidence between member states and that future cooperation will be undermined by improper use or privacy breaches.<br><br>The Terms of Use should provide the following minimum safeguards:<br>• Suspension or cancellation of participation if there is a breach of any rules.<br>• Expectation that countries will take appropriate action against officials who misuse the Technical Solution. |
| If the cost of using the Technical Solution is high, the use of the Technical Solution may be limited. | End user interfaces should remain relatively simple and cost effective to ensure there is limited cost overheads for users, particularly in terms of both technology and training. |
| Safeguards should be established to ensure that data sharing does not breach international human rights obligations, such as those under the non-refoulement principle and the Universal Declaration of Human Rights, and where applicable, the Refugees Convention, the International Covenant on Civil and Political Rights, the Convention Against Torture, the Convention on the Right of the Child, and the Convention on Transnational Organized Crime.<br><br>The Technical Solution should also not be used to discriminate against groups of people without fair and reasonable cause. | The Terms of Use should provide the following minimum safeguards:<br>• Safeguards should be available to all individuals, regardless of whether they are a citizen or national of a member state.<br>• Biometric data of an individual who has sought asylum, made a claim of torture, cruel, inhumane or degrading treatment, and/or been recognized as a refugee is not transferred to a country of origin or feared harm (without their express consent).<br><br>Countries may explore further safeguards such as:<br>• Where there is consent, countries should be able to send information to UNHCR if there is a claim of prior asylum, or if there is a suspicion that a person has previously sought asylum with the UNHCR (where consent is granted).<br>• Biometric data of an individual who has sought and/or received protection is not transferred to a country where there is an unacceptable risk of that information being disclosed to an agent of persecution or significant harm. |

| | |
|---|---|
| | • Considerations for vulnerable persons, such as women, children and victims of trafficking.<br><br>The Technical Solution may incorporate these minimum safeguards into business rules, header information and preliminary questions for users. |
| Responsibilities, standards and safeguards under the Framework may lead to officials breaching domestic laws, for example data retention laws. | The Terms of Use should clearly establish that the use of the Framework will only be subject to the domestic laws, policies and international obligations of participating members. |
| Officials must have the domestic legal authority to collect, use and disclose biometric data to protect against the unlawful exercise of powers. | The bilateral elements of the Framework can flexibly accommodate member states' different needs for legal authority. For example, depending on the member state's circumstances, a bilateral agreement can be legally binding and act as a source of legal authority to collect, use and disclose biometric data. |
| Since personal information will be shared, there should be safeguards for personal privacy and data protection. Safeguards will need to take into account domestic privacy and data protection laws and policy, while also ensuring that minimum safeguards are met. | The Terms of Use should include minimum privacy and data protection safeguards that are broadly consistent with privacy principles set out in the OECD Guidelines and the APEC Framework, the most widespread and accepted privacy principles in the region.<br><br>Additional safeguards can be added in bilateral agreements as per the needs of individual bilateral relationships.<br><br>The Technical Solution may also incorporate privacy safeguards into its business rules. |
| The risk of a breach of the data system (for example through human error or hacking) is one of the most significant risks of data sharing. Unauthorized disclosure to third parties can also jeopardize the law enforcement function. | The Terms of Use should provide the following minimum safeguards:<br>• data security and accountability<br>• data should be retained for only the period necessary for identification purposes.<br><br>Member states should notify the other country of any security breaches, and where appropriate, the data subject. |
| Information should be collected by lawful and fair means, and where appropriate, with the consent of the individual. This is consistent with the collection principles under the OECD Guidelines and the APEC Framework and is a necessary check on government power. This not only | The Terms of Use should provide the following minimum safeguards:<br>• Information should only be collected by lawful and fair means, with clear notice (either generally or specifically) of the purpose of the collection and intended use.<br><br>Member states can also consider: |

| | |
|---|---|
| protects personal privacy but also reduces the risk of information being used for improper purposes and strengthens the legality of potential law enforcement investigations. Unlawful collection results in officials acting outside of their legal authority and breaching the rule of law. | • Training officials to clearly understand their lawful authority.<br>• In addition to seeking specific consent from an individual, general notices can be shown at the time of collection.<br>• Awareness campaigns that create general understanding of the Framework for individuals. |
| Use and disclosure of information should be consistent with the purpose notified to the individual at the time of collection, unless there is subsequent consent of the individual or authority from the law. This is consistent with the purpose specification and use limitation principles under the OECD Guidelines and APEC Framework. | The Terms of Use should provide the following minimum safeguards:<br>• The use and disclosure of information should be consistent with the purpose notified to the individual at the time of collection, unless there is subsequent consent or authority from the law.<br><br>Member states can also consider:<br>• Exploring how, under their domestic laws, officials can have specific lawful authority and exemptions to use and disclose information in a way that is not consistent with the purpose notified.<br>• Personal information should only be matched with data that was obtained for an identification, nationality, law enforcement, people smuggling, migration, trafficking in persons or related transnational crime purpose. |
| Reliance of inaccurate information undermines the integrity of the data sharing system and can potentially have severe adverse effects on individuals. Inaccurate data could result in mis-identification and in innocent individuals being charged, detained or convicted.<br><br>Further, inaccurate data from one database can be replicated in other databases.<br><br>If data is shared with countries that do not allow access and correction of data, it may be impossible for individuals to correct the inaccurate personal information stored. | The Terms of Use should provide the following minimum safeguards:<br>• Data should be accurate, complete and up-to-date.<br>• Data should be retained for only as long as needed for the purpose for which it is used.<br>• Officials and individuals should have available to them avenues to access and correct the personal information that exists within any database.<br>• Members should notify relevant members to any inaccurate information and seek to amend or correct that information. |
| Data should be non-identifiable | Depersonalized and non-identifiable data should be shared |

| | |
|---|---|
| wherever possible. This not only protects the privacy of individuals, but also minimizes harm caused by breaches of the system.<br><br>While data needs to be identifiable for officials to verify identity, the risk of inadvertent or improper disclosure to third parties means that the data itself should not be personally identifiable. | wherever possible. This means that officials should consider using only one biometric data in the one request – they should be separated if possible. |
| Some countries have avenues for third parties to access information through court processes and rights to government information. Inquiries and royal commissions may also have powers to compulsorily obtain information. Release of information through these avenues may breach privacy protections. | Member states may consider inserting confidentiality obligations in bilateral agreements to protect both the privacy of individuals and the integrity of the investigative process. While this might not be legally binding or may be ultimately overridden by more binding or coercive laws, such obligations should ensure that confidentiality and privacy concerns are adequately considered. |

## Attachment B: Example Terms of Use

### Background

At the 6th Ministerial Conference of the Bali Process, the Ministers of the Bali Process member states:

- Recognizing the importance of burden sharing, collective responsibility and international and regional cooperation to combat irregular migration, people smuggling, trafficking in persons and related transnational crimes;
- Desiring to facilitate cooperation between Bali Process members through the timely sharing of biometrics for the purposes of identity verification and combating identity fraud;
- Respecting the importance of confidentiality and upholding the human rights and privacy of individuals;
- Noting that it is not intended for these Terms of Use to be legally binding or to displace the domestic laws, policies and international obligations of a Participating Member;
- Noting that the use of the Technical Solution under these Terms of Use should complement and not prejudice any other information sharing mechanism available to Bali Process members; and
- Noting that the Technical Solution under these Terms of Use forms part of a greater context of general information sharing among Bali Process members;

Endorsed the establishment of the Technical Solution under these Terms of Use.

### Definitions

1. Definitions:
   (a) Biometrics means the automated recognition of individuals based on their biological and behavioral characteristics, and includes facial images, fingerprints and iris and retina scans.
   (b) Individual means any natural person, whether they are a citizen or non-citizen, or a national or non-national of a country.
   (c) Personal information means any information that may, by itself or with other information, be used to identify an individual, and includes biometrics.
   (d) Participating Member means any Bali Process member state or organization that has complied with paragraphs 4 and 5 of these Terms of Use.
   (e) Requesting Member means the Bali Process member state or organization that makes a request under paragraph 10 of this Terms of Use.
   (f) Responding Member means the Bali Process member state or organization that makes a response under paragraph 11 of this Terms of Use.
   (g) Technical Solution means the technological mechanism established to facilitate the exchange of biometric data between Participating Members under these Terms of Use.

### Scope of the engagement

2. The use of the Technical Solution is intended to be limited to identification and identity verification for irregular migration, people smuggling, trafficking in persons and related transnational crime purposes only.

## Participation and reporting

3. All Bali Process member states and organizations are entitled to participate and use the Technical Solution. Use of the Technical Solution is voluntary and is subject to the domestic laws, policies and international obligations of Participating Members.

4. Use of the Technical Solution is conditional upon Participating Members agreeing with each other in writing the specific details of data sharing arrangements. The agreement must be consistent with these Terms of Use, and to the extent of any inconsistency, these Terms of Use shall prevail. Any agreement may provide additional safeguards to the minimum safeguards provided under these Terms of Use. Agreements under this paragraph should specify:
    a. The type of biometric data to be shared
    b. Any other information, including personal information, to be shared
    c. The biometric databases in which biometric data will be matched
    d. The maximum time period for which a response can be given referred to in paragraph 10
    e. The national manager referred to in paragraph 17
    f. The security mechanisms in place, including details of data retention referred to in paragraph 23
    g. Other safeguards additional to the minimum protections in paragraphs 14-23
    h. Any other operational procedures to be followed

5. Participation will be accepted by the RSO upon written notification that members have made an agreement consistent with paragraph 4 above.

6. A committee established by Senior Officials of the Bali Process Ad Hoc Group, (the Committee) consisting of no less than 5 Ad Hoc Group members and supported by the RSO, will be the primary body responsible for administrative and oversight purposes. Participation may be suspended or cancelled by the Committee if it is satisfied that a Participating Member has breached a term of these Terms of Use. The RSO, upon being notified in writing of any possible breach of these Terms of Use, may decide to temporarily suspend the participation of the Participating Member involved until a decision has been made by the Bali Process Ad Hoc Working Group.

7. Questionnaires and confidential reports may be periodically produced about the use of the Technical Solution. Information contained in any reports and questionnaires will not be released without the prior written consent of the Participating Member that provided the information.

8. Participating Members are expected to take appropriate action, including under the civil or criminal law or both of the domestic law, in the event of misuse of the Technical Solution or unauthorized use and disclosure of personal information under these Terms of Use.

## Information sharing

9. Wherever possible, to reduce the risk of inaccuracies or overdependence on biometrics, it is intended that multiple sources of information be used to identify or verify the identity of individuals.

10. The Requesting Member shall make a request by sending a biometric through the Technical Solution (Request Tool). Requests will stay active until there is a response or until the request period expires. The length of the request period shall be agreed between the Participating Members but may not be for more than 5 working days.

11. The Responding Member may respond to a request by returning a “match” or “no match” response.

12. Where a request is made under paragraph 10 or a response is returned under paragraph 11, the Participating Members must make a record of that transaction.

13. A Responding Member may refuse to respond to a request for any national security, public health or public policy reason, including that a response may be incompatible with the Responding Member’s domestic laws and policy. Wherever possible, the Responding Member should notify the Requesting Member of the refusal and provide reasons where appropriate.

### Human rights protections

14. Wherever possible, Participating Members are expected to not draw adverse inferences or take adverse action against an individual merely because of the fact that a request for information sharing has been made or that a match has been made.

15. If an adverse action is made against an individual that was made, partially or wholly, on the basis of information shared through the Technical Solution, it is expected that the affected individual be notified and have the opportunity to comment on the information.

16. If an individual has raised a claim of persecution, torture or cruel, inhumane or degrading treatment against a country or government agency of a country, Participating Members must not share information about that individual with that country, unless it has that individual’s express written consent to do so.

### Data protection

17. Personal information collected from and used through the Technical Solution is expected to be maintained in secure systems that are protected from loss or unauthorized access, destruction, use, modification or disclosure. The system should have a minimal number of authorized users. The Participating Member must appoint a National Manager who acts as a central focal point for requests and responses made through the Technical Solution. The National Manager will be responsible for the operation of the network in a way consistent with these Terms of Use.

18. Collection of personal information is expected to be by lawful and fair means. Wherever possible, individuals will be notified of the identity verification purpose for which their personal information has been or will be collected.

19. Wherever possible, taking into account the confidential nature of law enforcement and border management processes, it is expected that the consent of the individual should be obtained prior to the collection, use and disclosure of their personal information.

20. It is expected that use and disclosure of personal information should be consistent with the purpose notified to the individual at the time of collection, unless there is subsequent consent from the individual or authority from the law. Personal information should only be matched with data that was obtained for an identification, nationality, law enforcement, people smuggling, migration, trafficking in persons or related transnational crime purpose.

21. To the greatest extent possible, information about individuals should be complete, accurate and up to date. Individuals should be given the opportunity to access and correct their personal information. Participating Members are expected to inform relevant parties about any inaccurate information shared and seek to correct that information.

22. Personal information will not be disclosed to a third party without the consent of the Participating Member that provided that personal information. The Participating Member providing that personal information may place restrictions on use and disclosure of that information, and it is expected that other participating members comply with such restrictions.

23. It is expected that personal information will only be retained for as long as it is necessary to verify the identity of an individual. Personal information should be deleted as soon as it is no longer necessary for this purpose, in accordance with the relevant Participating Member's domestic law and policy.

**Final paragraphs**

24. Each Participating Member will bear their own costs of their use of the Technical Solution.

25. These Terms of Use may be amended through the endorsement of the Bali Process member states following a recommendation by the Committee established under paragraph 6 of these Terms of Use.

26. The protections and safeguards contained in paragraphs 14-23 of these Terms of Use and any additional protections and safeguards made under any agreement under paragraph 4 shall survive any suspension or cancellation of a Participating Member's participation in the Technical Solution and any termination of any agreement made under paragraph 4 of these Terms of Use.

27. All disputes under these Terms of Use, including any arising from any agreements made under paragraph 4 above, shall be settled amicably through consultation or negotiation between the Participating Members concerned through diplomatic channels, without reference to any third party or international tribunal.