Disposition of Comments: Privacy Final Recommendation V1.0									
Reference	**Conformance Criteria**	**Level of Assurance (LOA)**							
BASE	**Baseline** **Note:** *Requirements for use cases where the Subject acts as the Disclosing Organization are not addressed in this version of the Baseline conformance criteria.*	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Comment**	**Final Recommendation**	**Accepted, Deferred, or Rejected**	**Deemed Auditable**
1	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Facilitator and the Governing Body **MUST** have a privacy management program in place to ensure compliance with applicable law including the implementation of privacy policies, practices, controls and assessment tools.						Disclosing Organizations, Requesting Organizations, Network Facilitators, and Notice and Consent Processors MUST have in place an appropriate privacy management program that documents policies, practices and procedures to comply with applicable privacy laws, and incorporates the following: - What information they collect, use, keep and disclose and why - Privacy risk assessment - Individual rights, complaints and questions - Any relevant restrictions on collection, use, retention or disclosure (legal, contractual) - Training and awareness - Diligence on third parties (includes customer, suppliers, service providers, partners) - Security measures and incident response and management - Information about cross-border transfer of personal information	Accepted as Noted	Yes, with changes
2	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Facilitators and the Governing Body **MUST** have a designated privacy official who is responsible for overseeing the privacy management program and any internal audits or reviews of personal information handling practices (including those related to the provision of notice and the obtaining of consent).					**Applicable for all conformance criteria.** For mitigating risks, clients implement controls. Consider adding controls supporting each conformance criteria which would include details around what needs to be validated and how? This can be further supported by including examples of (1) artifacts/evidence and (2) audit procedures	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Facilitators and the Governing Body **MUST** have a designated privacy official who is responsible for overseeing the privacy management program and any internal ~~audits or~~ reviews of personal information handling practices (including those related to the provision of notice and the obtaining of consent), and has the authority to intervene on privacy issues specifically relating to the organization's role as a Disclosing Organization, Requesting Organization, or Notice and Consent Processor.	Accepted as Noted	Yes
3	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Facilitators and the Governing Body **MUST** have a comprehensive privacy policy that: - provides a description of its personal information handling practices; and - is easily accessible, simple to read, and updated as required.							Accepted	Yes
4	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Facilitators and the Governing Body **MUST** periodically audit or perform a review of their personal information management practices (including its notice and consent management practices), to a maximum of 3 years between audits or reviews, to ensure that Personal Information is being handled in the way described by its privacy policy.					"Less ambiguity: ""MUST periodically perform a review"" (remove ""or"") Is it by internal or external means at the discretion of the organization?"	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Facilitators and the Governing Body **MUST** periodically ~~audit or~~ perform an Independent internal or external review of their personal information management practices (including its notice and consent management practices), to a maximum of ~~3 years~~ 1 year ~~between audits or~~ reviews, to ~~ensure~~ verify that Personal Information is being handled in the way described by its privacy policy.	Accepted as Noted	Yes
5	The Governing Body **MUST** ensure organizations operating within the Digital Identity Ecosystem comply with the conformance criteria listed for Principles 1-10.						Participants **MUST** maintain evidence of compliance to the conformance criteria for Principles 1-10, which can be provided to other participants, including the Governing Body, when requested.	Accepted as Noted	Yes
6	As part of their privacy management programs, Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Facilitators and the Governing Body **MUST** have processes to manage Personal Information breaches or breaches of confidentiality, which includes assessing damage or harm, reporting, containment, remediation, notification, and prevention steps.						As part of their privacy management programs, Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Facilitators and the Governing Body **MUST** have and periodically test processes to manage Personal Information breaches or breaches of confidentiality, which includes ~~s~~ assessing damage or harm (for organizations and individuals), reporting, containment, remediation, notification, and prevention steps.	Accepted as Noted	

7	The Governing Body **MUST** clearly define and manage the boundaries of the Digital Identity Ecosystem					A4 Each organisation has to set out their role in the digital identity ecosystem and to agree in writing between the relevant organisations who has what responsibilities with regards to user personal information. This must cover: -whether consent is required and any requirements for the form and manner of the consent; -restrictions on use and disclosure; -data sharing; - user rights; -transparency obligations; -consent obligations if appropriate; -security obligations; and -data deletion arrangements.	The Governing Body **MUST** clearly define, document and manage the boundaries of the Digital Identity Ecosystem	Accepted as Noted	Yes, by adding "document"
Reference	**Conformance Criteria**	**Level of Assurance (LOA)**							
ACCO	**Principle 1 - Accountability** **Note:** *An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles.*	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**If "No", please recommend adjustment**	**Final Resolution/Next Steps**	**Accepted, Deferred, or Rejected**	**Deemed Auditable**
Process/Function Overview:									
1	Disclosing Organizations, Requesting Organizations, Network Facilitators, and Notice and Consent Processors **MUST** ensure the User has a clear idea of who (e.g. designation, contact information) is responsible for privacy in their respective organizations.					A2 Each organisation must have one or more people who are responsible and have authority for privacy matters and publicly-available contact details to reach those people.	REMOVE. Repeat of updated BASE-1, that incorporates ACCO 3,5,6 and 7	Accepted as Noted	Yes
2	Disclosing Organizations, Requesting Organizations, Network Facilitators, and Notice and Consent Processors **MUST** make the name or title of the person who is responsible for privacy in their respective organizations readily available to the User and provide them with the means to contact that person.					Criteria 1 and 2 could be merged	Unchanged as ACCO-1 removed.	Accepted	Yes
3	The Disclosing Organization **MUST** have a privacy management program that includes: - if applicable, restrictions based on the type of organizations with whom the Subject-Specific Personal Information will be shared or restrictions based on the purpose for collecting that information. For example, there may be restrictions based on sector or regulatory environment (e.g., health, financial services); - if applicable, specification of the requirements to be met by relevant Digital Identity Ecosystem participants regarding the handling of a Subject-Specific Personal Information; - if applicable, restrictions on the process of sharing the Subject-Specific Personal Information; - processes to be followed when the Subject-Specific Personal Information is shared; - processes to be followed when the Subject-Specific Personal Information previously shared is updated, deleted or expired; - clear guidance for Users on the sharing of the Subject-Specific Personal Information to help them know which party they should contact depending on the nature of their inquiry; - data protection controls; and - privacy impact assessment that explicitly covers the disclosure of the Subject-Specific Personal Information through the Digital Identity Ecosystem.						REMOVE. Rendered redundant by updated BASE-1, that incorporates ACCO 3,5,6 and 7	Accepted as Noted	Yes
4	Disclosing Organizations, Requesting Organizations, and Notice and Consent Processors **MUST** ensure that the responsibilities of their designated official include the authority to intervene on privacy issues specifically relating to the organization's role as a Disclosing Organization, Requesting Organization, or Notice and Consent Processor. This may be delegated but the original processor remains accountable. This will ensure a holistic and consistent approach to the protection of the Subject's privacy.						REMOVE. Updated BASE-2 description of privacy offical responsibilities.	Accepted as Noted	Yes

5	The Requesting Organization **MUST** have a privacy management program that includes: - if applicable, restrictions based on the type of organizations from whom the Subject-Specific Personal Information will be obtained or restrictions based on the purpose for collecting that information. For example, there may be restrictions based on sector, regulatory environment (e.g., health, financial services); - if applicable, processes to be followed when the Disclosing Organization defines specific requirements to the Requesting Organization regarding the handling of Subject-Specific Personal Information; - if applicable, restrictions on the process of obtaining the Subject-Specific Personal Information; - processes to be followed when the Subject-Specific Personal Information is obtained via the digital identity system; - processes to be followed when the Subject-Specific Personal Information previously obtained is updated, deleted or expired; - clear guidance for Subjects on the sharing of data to help them know which party they should contact depending on their inquiry; - data protection controls; and - privacy impact assessment that explicitly covers the use of the Subject-Specific Personal Information obtained through the Digital Identity Ecosystem. Suggest limiting the Notice & Consent Processor's responsibility to changes that affect the Subject's stored consent directive state. Suggest change as follows: "previously shared is updated, deleted or expired. The Notice & Consent Processor must have processes in place to manage changes affecting the Subject's stored consent directive, specifically the consent directive's state."						REMOVE. Rendered redundant by updated BASE-1, that incorporates ACCO 3,5,6 and 7	Accepted as Noted	Yes
6	The Notice and Consent Processor **MUST** have a privacy management program that includes: - restrictions on use of Personal Information where the Notice and Consent Processor is just a facilitator, for example, the Notice and Consent Processor should never be in possession of or store the Subject-Specific Personal Information; - if applicable, processes to be followed when the Disclosing Organization defines specific requirements to the Notice & Consent Processor regarding the handling of Subject-Specific Personal Information; - processes to be followed when facilitating the sharing of the Subject-Specific Personal Information; - processes to be followed for the management of consent by the Subject - processes to be followed when the Subject-Specific Personal Information previously shared is updated, deleted or expired; - clear guidance for Subjects on the sharing of the Subject-Specific Personal Information to help them know which party they should contact depending on the nature of their inquiry; - data protection controls; and - privacy impact assessment that explicitly covers the facilitation role, focusing on minimizing (or even eliminating) access to or visibility of the Subject-Specific Personal Information or Service-Specific Information.						REMOVE. Rendered redundant by updated BASE-1, that incorporates ACCO 3,5,6 and 7	Accepted as Noted	N/A
7	The Network Facilitator **MUST** have a privacy management program that includes: - restrictions on use of Personal Information where the Network Facilitator is just a facilitator, for example, potentially the Network Facilitator must never be in possession of, or store, the Subject-Specific Personal Information; - if applicable, processes to be followed when facilitating the sharing of the Subject-Specific Personal Information; - processes to be followed when the Subject-Specific Personal Information previously shared is updated, deleted or expired; - clear guidance for Subjects on the sharing of the Subject-Specific Personal Information to help them know which party they should contact depending on the nature of their inquiry; - data protection controls; and privacy impact assessment that explicitly covers the facilitation role, focusing on minimizing (or even eliminating) access to or visibility of the Subject-Specific Personal Information or Service-Specific Information.						REMOVE. Rendered redundant by updated BASE-1, that incorporates ACCO 3,5,6 and 7	Accepted as Noted	N/A

8	The Governing Body **MUST**: - ensure accountability of the organizations operating with the Digital Identity Ecosystem; - If applicable, ensure that specific requirements defined by an organization on a Subject-Specific Personal Information are complied with by relevant Digital Identity Ecosystem participants; - include rules concerning standards and interoperability that ensure all parties involved in the sharing of the Subject-Specific Personal Information treat the Subject and the Subject-Specific Personal Information in a consistent and compatible way; - include procedures to investigate and manage privacy breaches, including assessing the risk to individuals and reporting breaches to relevant privacy regulators and individuals; and facilitate monitoring of operational risks (e.g., fraud, information security) across the Digital Identity Ecosystem.						The Governing Body **MUST** define procedures that: - investigate and manage deviations from Principles 1-10 by organizations operating within the Digital Identity Ecosystem, including assessing the risk to Subjects and reporting breaches to relevant privacy regulators and Subjects - If applicable, ensure verify that specific requirements defined by an organization on a Subject-Specific Personal Information are complied with by relevant Digital Identity Ecosystem participants - include rules concerning standards and interoperability that ensure all parties involved in the sharing of the Subject-Specific Personal Information treat the Subject and the	Accepted as Noted	Yes, after updates
Reference	**Conformance Criteria**	**Level of Assurance (LOA)**							
IDEN	**Principle 2 - Identifying Purposes** **Note:** *The purposes for which the personal information is being collected must be identified by the organization before or at the time of collection.*	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**If "No", please recommend adjustment**	**Final Resolution/Next Steps**	**Accepted, Deferred, or Rejected**	**Deemed Auditable**
Process/Function Overview:									
1	The Disclosing Organization **MUST** have confidence that Principle 2 is being followed by Requesting Organizations and Notice and Consent Processors before disclosing Personal Information to those organizations.						Replace with more auditable verbiage: The Disclosing Organization **MUST** be able to demonstrate that sufficient due diligence was performed over the existence of relevant governance or control-processes at Requesting Organizations and Notice and Consent Processors, before disclosing Personal Information to those organizations.	Accepted as Noted	Yes
2	The Disclosing Organization **MUST** maintain and preserve a timeline of retrievable documentation for records of information requests and disclosure events. The timeline may consist of a single event (a "one-time request and disclosure"), or multiple events depending on the circumstances of the exchange.						change "for records of" to "that includes"	Accepted as Noted	Yes
3	The Requesting Organization **MUST** clearly identify the purpose for collecting Subject-Specific Personal Information through the Notice and Consent Processor.						The Requesting Organization **MUST** have a clear, defined, justifiable identity-related purpose...	Accepted as Noted	Yes
4	The Requesting Organization **MUST** maintain and preserve a timeline of retrievable documentation for why Personal Information is needed and how it will be used.						No changes	Accepted	Yes
5	The Requesting Organization **MUST** periodically, to a maximum of 3 years between reviews, perform an internal review of their Personal Information collection and use requirements, and update future requests accordingly.						Change to 1 year.	Accepted as Noted	Yes
6	The Requesting Organization **MUST** ensure that the reasons for the collection and use of Subject-Specific Personal Information are clear, unambiguous, and not overly broad.						The Requesting Organization **MUST** ~~ensure~~ verify that the reasons for the collection and use of Subject-Specific Personal Information are clear, specific, and unambiguous, ~~and not overly broad~~.	Accepted as Noted	yes, after updates.
7	Before or when any Personal Information is collected, the Notice and Consent Processor **MUST** explain in writing to the Subject why it is needed and how it will be used.						Replace "in writing" with "explicitly"	Accepted as Noted	Yes
8	The Governing Body **MUST** clearly define the scope of the Digital Identity Ecosystem to all participants and that identifying purposes beyond the scope of the Digital Identity Ecosystem (which may exist within each participating organization) are not covered.						REMOVE. Replaced by updated BASE-5, and ACCO-8	Accepted as Noted	Yes
9	The Governing Body **MUST** ensure organizations operating within the Digital Identity Ecosystem comply with the conformance criteria listed for Principles 2, and evidence of the Requesting Organizations compliance can be provided to Disclosing Organizations.						Replace "ensure" with "verify that" - might already be covered by blanket statement.	Accepted as Noted	Yes
10	The Governing Body **MUST** include procedures to investigate and address deviations from Principle 2.						REMOVE. Replaced by updated BASE-5, and ACCO-8	Accepted as Noted	N/A
Reference	**Conformance Criteria**	**Level of Assurance (LOA)**							
CONS	**Principle 3 - Consent** **Note:** *The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.*	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**If "No", please recommend adjustment**	**Final Resolution/Next Steps**	**Accepted, Deferred, or Rejected**	**Deemed Auditable**
Process/Function Overview:									

1	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** ensure the notice and knowledge required for the consent request is clear, understandable and meaningful to the User.						Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** ~~ensure~~ verify that the notice and knowledge required for the consent request is clear, understandable and meaningful to the User, and include details to indicate if the consent is one-time only or ongoing, and how the User may revoke or withdraw the consent. See also NOTI 1, 3, 4 and 5, CONS-8 and MANA-2 and 6 in the	Accepted as Noted	Yes
2	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **SHOULD** ensure the consent process balances sufficient information to the User against information overload. In all cases, a straightforward means **SHOULD** be provided for the User to get additional information, as may be required.						Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **SHOULD** ensure the consent process is clear as to what is being consented to. ~~balances sufficient information to the User against information overload~~. In all cases, a straightforward means **SHOULD** be provided for the User to get additional information, as may be required.	Accepted as Noted	Yes
3	The Disclosing Organization **MUST** ensure the Notice and Consent Processor performs its function of providing notice and recording/managing consent appropriately prior to disclosing the Subject-Specific Personal Information.					If the notice and consent procssor is appointed to the task by the disclosing organization. But if they're independent, who does the verification of their compliance?	Updated with reference and verbiage matching Notice and Consent component. Merged with CONS-10 as per recommendation. The Disclosing and the Requesting Organizations **MUST** ~~ensure~~ verify that the Notice and Consent Processor performs its function of providing notice, and obtaining, recording and managing consent appropriately prior to disclosing or receiving the Subject-Specific Personal Information. Both the Disclosing and the Requesting Organizations MUST ensure that the consent is in place before providing it or before receiving it. See also NOTI-1 in the PCTF Notice and Consent component.	Accepted as Noted	Yes
4	The Disclosing Organization **MUST** ensure that evidence of the notice and consent is obtained by the Notice and Consent Processor and then stored appropriately.						The Disclosing Organization **MUST** ~~ensure~~ verify that evidence of the notice and consent is obtained by the Notice and Consent Processor and then stored ~~appropriately~~ as a Notice and Consent record.	Accepted as Noted	Yes, after updates
5	The Disclosing Organization **MUST** confirm notice and consent is not expired or revoked at the time of sharing a Subject-Specific Personal Information. In the event the consent is not expired or revoked, the Requesting Organization **MUST** be provided with a response that indicates the consent is valid.						Change "confirm" to "verify"	Accepted as Noted	yes
6	The Disclosing Organization **MUST** ensure the User has access to the information required to understand the nature, purpose, and risks associated with the use or disclosure, of their Subject-Specific Personal Information, within the Digital Identity Ecosystem. For example, via the Privacy notice statement. See also **NOTI-5** in the PCTF Notice and Consent component.						No changes	Accepted	yes
7	The Requesting Organization, as the originator of the request for consent, **MUST** be responsible for defining the purpose of processing the requested Subject-Specific Personal Information in the content of the notice. See also **NOTI-5** in the PCTF Notice and Consent component.						Reference is to NOTI-3, not 5.	Accepted as Noted	yes
8	The Requesting Organization as the originator of the request for consent, MUST be primarily responsible for defining the nature of the sharing request in the content of the notice. Note: Nature of sharing refers to whether the request is for a one-time disclosure of the personal information or to allow on-going disclosure.						The Requesting Organization as the originator of the request for consent, **MUST** ~~rprimarily be responsible for~~ define whether the request is for a one-time disclosure of the personal information or to allow on-going disclosure ~~the nature of the sharing request~~ in the content of the notice. ~~Note: Nature of sharing refers to whether the request is for a one-time disclosure of the personal information or to allow on-going disclosure.~~ See also NOTI-3 in the PCTF Notice and Consent component.	Accepted as Noted	yes
9	The Requesting Organization **MUST** ensure that the request follows a principle of minimal disclosure.						Clarify that the request it is the consent request.	Accepted as Noted	yes

10	The Requesting Organization **MUST** ensure the Notice and Consent Processor performs its function of providing notice and recording/managing consent appropriately prior to receiving Subject-Specific Personal Information.					How can both the requesting and disclosing organizations be responsible for validating this requirement at the same time? Responsibility should lie with the organization that contracted the notification service.	REMOVE. Combined with CONS-3.	Accepted as Noted	N/A
11	The Requesting Organization **MUST** ensure that a record of the notice and consent is obtained by the Notice and Consent Processor and then stored appropriately.						The Requesting Organization **MUST** ~~ensure~~ verify that a record of the notice and consent is obtained by the Notice and Consent Processor and then stored ~~appropriately~~ as a Notice and Consent record.	Accepted as Noted	Yes, after updates.
12	When the Requesting Organization is made aware that consent is no longer valid, the Requesting Organization **MUST** cease further collection of Subject-Specific Personal Information based on this invalidated consent.						When the Requesting Organization is made aware that consent is no longer valid, the Requesting Organization **MUST** have a process to cease further collection of Subject-Specific Personal Information based on this invalidated consent. See also MANA-2 in the PCTF Notice and Consent component.	Accepted as Noted	Yes, after updates.
13	The Notice and Consent Processor **MUST** be responsible for providing notice to the User within the Digital Identity Ecosystem.						The Notice and Consent Processor **MUST** ~~be responsible for~~ provide notice to the User within the Digital Identity Ecosystem.	Accepted as Noted	Yes
14	The Notice and Consent Processor **MUST** ensure its notice clearly reflects the nature of sharing within the Digital Identity Ecosystem. Note: Nature of sharing refers to whether the request is for a one-time disclosure of the personal information or to allow on-going disclosure.						The Notice and Consent Processor **MUST** ~~ensure its~~ verify that the notice clearly states ~~reflects~~ ~~the nature of sharing~~ whether the request is for a one-time disclosure of the personal information or to allow on-going disclosure within the Digital Identity Ecosystem. ~~Note: Nature of sharing refers to whether the request is for a one-time disclosure of the personal information or to allow on-going disclosure.~~	Accepted as Noted	Yes
15	The Notice and Consent Processor **MUST** ensure, or receive confirmation, the User is authenticated prior to displaying any Subject-Specific Personal Information within a notice to the User by validating the identity of the User.						No changes	Accepted	Yes
16	The Disclosing Organization **MUST** define the sensitivity of the Personal Information being shared and implement their rules (e.g., masking policies) for the display of sensitive information within the notice.						The Disclosing Organization **MUST** define the sensitivity of the Personal Information being shared and define and stipluate controls ~~rules~~ (e.g., masking policies and other safeguards) for the display of sensitive information within the notice.	Accepted as Noted	Yes
17	The Notice and Consent Processor **MUST** be able to display Personal Information in the notice in accordance with any rules (e.g., masking policies) stipulated by the Disclosing Organization.						The Notice and Consent Processor **MUST** be able to display Personal Information in the notice in accordance with any controls ~~rules~~ (e.g., masking policies or other safeguards) stipulated by the Disclosing Organization.	Accepted as Noted	Yes
18	The Notice and Consent Processor **MUST** provide a means to collect consent and communicate this to the other parties involved in the digital identity transaction (Disclosing Organization and Requesting Organization).						The Notice and Consent Processor **MUST** have a process ~~provide a means~~ to collect consent and communicate this to the Disclosing Organization and Requesting Organization involved in the digital identity transaction. ~~(Disclosing Organization and Requesting Organization)~~.	Accepted as Noted	Yes
19a	The Notice and Consent Processor **MUST** record the consent and provide the User with means to review and manage any consents given.						Two criteria here with a MUST and a SHOULD. The Notice and Consent Processor **MUST** record the consent decision. See also RECO-1 in the PCTF Notice and Consent component.	Accepted as Noted	Yes
19b	New						The Notice and Consent Processor **SHOULD** have a straightforward process for the User ~~means~~ to review and manage any consents given. See also MANA 7 in the PCTF Notice and Consent component.	Accepted as Noted	Yes
20	For identity transactions where consent is being managed between multiple Requesting Organizations and Disclosing Organizations, the Notice and Consent Processor **MUST** ensure all organizational boundaries are maintained and/or preserved.						For identity transactions where consent is being managed between multiple Requesting Organizations and Disclosing Organizations, the Notice and Consent Processor **MUST** ensure ~~all organizational boundaries are maintained and/or~~ that processing is conducted in accordance with the purpose specified in the Notice and the consent granted by the User for each organization.	Accepted as Noted	Yes, after updates

21	The Notice and Consent Processor **MUST** have processes in place to support the revocation of consent. For example, an action to revoke consent could originate from the Subject or be in response to the detection of fraudulent activity by any one of the digital identity processing organizations.						The Notice and Consent Processor **MUST** have processes ~~in place~~ to support the revocation of consent. For example, an action to revoke consent could originate from the Subject or be in response to the detection of fraudulent activity by any one of the digital identity processing organizations. See also MANA-3, 4 and 5 in the PCTF Notice and Consent component.	Accepted as Noted	Yes
22	The Network Facilitator **MAY** be involved in determining or discovering which Disclosing Organizations are potential sources of the requested Personal Information. Note: As an alternative, for example, Requesting Organizations may directly specify the required source.						This is a guideline or recommendation, rather than a autitable criteria.	Accepted as Noted	No, but can leave as guidance.
23	The Network Facilitator **MUST NOT** have visibility to unprotected Personal Information shared through the Digital Identity Ecosystem. Specifically, this includes any Personal Information presented in the notice and consent process, as well as transmission of Personal Information through the network.						No change	Accepted	Yes
24	The Governing Body **MUST** provide guidelines on the formulation of notices and collection of consent, to provide a consistent and optimized user experience across the Digital Identity Ecosystem.						Change "provide" to "define"	Accepted as Noted	Yes
25	The Governing Body **MUST** include procedures to investigate and manage deviations from Principle 3, including assessing the risk to Subjects and reporting breaches to relevant privacy regulators and Subjects.						REMOVE Merge to be part of BASE-5/ACCO-8, along with IDEN-10, CONS-25, and part of ACCO-8)	Accepted as Noted	N/A
26	The Governing body **MUST** include provisions which ensure that revocation of consent by a User is promptly effective across the entire Digital Identity Ecosystem.						The Governing body **MUST** ~~include define provisions which that~~ ensure that revocation of consent by a User is promptly effective across the entire Digital Identity Ecosystem.	Accepted as Noted	Yes
Reference	**Conformance Criteria**	**Level of Assurance (LOA)**							
LIMC	**Principle 4 - Limiting Collection** **Note:** *The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means.*	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**If "No", please recommend adjustment**	**Final Resolution/Next Steps**	**Accepted, Deferred, or Rejected**	**Deemed Auditable**
Process/Function Overview:									
1	The Disclosing Organization **MUST** have confidence that the Requesting Organization has good and sufficient reason for collecting the requested Personal Information.					L2 Business identity providers and third-party data providers must do appropriate diligence to make sure that Relying parties have a clear, defined, justifiable identity-related purpose	The Disclosing Organization **MUST** ~~have confidence~~ establish a process to verify that the Requesting Organization ~~has good and sufficient reason~~ has a clear, defined, justifiable identity-related purpose for collecting the requested Personal Information.	Accepted as Noted	Yes
2	The Requesting Organization **MUST** clearly delineate Personal Information collection activities via the Digital Identity Ecosystem from other activities of the Requesting Organization.					L10 Organisations can only use, keep and disclose the personal information for identity-related purpose(s). They cannot use that identity information for other unrelated purposes, such as marketing.	The Requesting Organization **MUST** only use, keep and disclose the Personal Information for identity-related purpose(s). They **MUST NOT** use that identity information for other unrelated purposes, such as marketing, *without consent* .	Accepted as Noted	Yes, after updates
3	The Requesting Organization **MUST** limit the Personal Information that is collected via the Digital Identity Ecosystem to what is necessary for the specific purpose of using the Digital Identity Ecosystem, e.g., to allow Users to access services or prove entitlement.					L3 Organisations collecting personal information from individuals can only collect the minimum information required to fulfill the stated identity-related purpose(s).	The Requesting Organization **MUST** limit the Personal Information that is collected via the Digital Identity Ecosystem to that which is required to fulfill the stated identity-related purpose(s).	Accepted as Noted	Yes
4	The Requesting Organization **MUST** publicly document, or make available, the kind and purpose of Personal Information collected.						The Requesting Organization **MUST** publicly document, or make available, in clear and unambiguous language the ~~kind~~ nature and purpose of Personal Information collected.	Accepted as Noted	Yes
5	The Requesting Organization **MUST** ensure that it educate applicable employees on the kind and purpose of Personal Information collected in order to accurately respond to any 3rd party inquiries.					Should tie last clause into an accountability statement around identifying an individual to respond to third party inquiries (as not any employee should do this)	The Requesting Organization **MUST** ~~ensure that it~~ educate applicable employees on the ~~kind~~ nature and purpose of Personal Information collected in order to accurately respond to any 3rd party inquiries **when they are required to do so.**	Accepted as Noted	Yes
6	The Requesting Organization **MUST** be clear, unambiguous, and transparent about the reason for collecting Personal Information in all forms of communication.						REMOVE. Merged with LIMC-4.	Accepted as Noted	N/A
7	The Notice and Consent Processor **MUST** ensure that Personal Information required to perform the notice and consent function is limited to only that which is required to perform the function.					Add "relevant" as Depending on their role, should be tailored to what is needed.	The Notice and Consent Processor **MUST** ~~ensure~~ verify that Personal Information being collected ~~required to perform the notice and consent function~~ is limited to only that which is required to perform the relevant notice and consent function.	Accepted as Noted	Yes
8	The Network Facilitator **MUST** facilitate the sharing of Personal Information.					Unclear what this would look like from an auditability standpoint – should be aligned to their service agreements and specific parties, and they should not be sharing PI for purposes different than authorized to the custodian	The Network Facilitator **MUST NOT** collect Personal Information beyond that which is required to support their service agreements. For example, acting on their behalf as a service or network provider.	Accepted as Noted	Yes

9	The Governing Body **MUST** have confidence that the Requesting Organization has good and sufficient reason for collecting the requested Personal Information.					L5 Organisations collecting personal information from individuals must make sure the collection is fair and lawful and they do not deceive or mislead individuals.	The Governing Body **MUST** ~~have confidence~~ have a process that would review the Requesting Organization's reason ~~that the Requesting Organization has good and sufficient reason~~ for collecting the requested Personal Information, and review that the collection is fair and lawful.	Accepted as Noted	Yes
10	The Governing Body **MUST** define rules and guidelines on appropriate ways to limit collection of Personal Information within and by the Digital Identity Ecosystem participants.						The Governing Body M**UST** ~~define~~ provide ~~rules and~~ guidelines on appropriate ways to limit collection of Personal Information within and by the Digital Identity Ecosystem participants.	Accepted as Noted	Yes
11	The Governing Body **MUST** include procedures to investigate and manage deviations from Principle 4, including assessing the risk to Subjects and reporting breaches to relevant privacy regulators and Subjects.						REMOVE - Combine into single statement for Principles 1-10.	Accepted as Noted	N/A
Reference	**Conformance Criteria**	**Level of Assurance (LOA)**							
LIMU	**Principle 5 - Limiting Use, Disclosure, and Retention** **Note:** *Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes.*	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**If "No", please recommend adjustment**	**Final Resolution/Next Steps**	**Accepted, Deferred, or Rejected**	**Deemed Auditable**
Process/Function Overview:									
1	The Disclosing Organization **MUST** have internal policies and other documentation for limiting use, disclosure, and retention of Subject-Specific Personal Information.						No Change	Accepted	yes
2	The Disclosing Organization **MUST** document uses of Subject-Specific Personal Information for the purpose of disclosure within the Digital Identity Ecosystem.						No Change	Accepted	yes
3	If there is a defined minimum and maximum data retention policy specified for the Digital Identity Ecosystem, the Disclosing Organization **MUST** comply with that policy with respect to the Subject-Specific Personal Information in connection with the Digital Identity Ecosystem. Note: Subject to regulatory restrictions.					L11 Organisations must have a retention schedule in place. Consumer identity providers should allow Individuals to decide how long they keep their card, account, wallet and so on. Business identity providers and Third-party data providers should set default retention periods, pass on any regulatory retention requirements to Relying parties and allow Relying parties to determine retention for the information relating to Individuals they are ID checking through the providers. Business identity providers and Third-party data providers must facilitate the Relying party determining their own retention for their own data.	~~If there is a defined minimum and maximum data retention policy specified for the Digital Identity Ecosystem,~~ The Disclosing Organization **MUST** comply with the defined minimum and maximum data retention policy, if specified, for the Digital Identity Ecosystem, ~~that policy~~ with respect to the Subject-Specific Personal Information in connection with the Digital Identity Ecosystem. Note: Subject to regulatory restrictions.	Accepted as Noted	yes
4	The Disclosing Organization **MUST** limit disclosure of the Subject-Specific Personal Information to only that required for the specific and intended purpose in alignment with Subject's consent, unless otherwise permitted or required by law.					L4 Organisations disclosing personal information must only disclose the minimum necessary for the identity-related purpose(s) and comply with any regulatory rules or relevant policies relating to masking.	The Disclosing Organization **MUST** limit disclosure of the Subject-Specific Personal Information to ~~only~~ that which is required to fulfill the stated identity-related purpose(s) ~~required for the specific and intended purpose~~ in alignment with Subject's consent, unless otherwise permitted or required by law.	Accepted as Noted	yes
5	The Disclosing Organization **MUST** limit disclosure of the Subject-Specific Personal Information to only that which the Disclosing Organization has confidence in the accuracy and currency of.					L6 Personal information collected, held, used or disclosed must be as accurate, complete, and as up-to-date as possible.	The Disclosing Organization **MUST** have processes in place to ensure that Personal Information to be disclosed is accurate, complete and as up-to-date as possible.	Accepted as Noted	yes
6	The Requesting Organization **MUST** document uses of Subject-Specific Personal Information received via the Digital Identity Ecosystem.						No change	Accepted	yes
7	Requesting Organizations and Notice and Consent Processors **MUST** institute maximum and minimum valid retention periods of the Subject-Specific Personal Information received via the Digital Identity Ecosystem.					See L11 comment on LIMU 3	Requesting Organizations and Notice and Consent Processors **MUST** implement maximum and minimum valid retention periods of the Subject-Specific Personal Information received via the Digital Identity Ecosystem, and be consistent with the retention specified in the Notice. See also NOTI-3 in the PCTF Notice and Consent component.	Accepted as Noted	yes
8	The Requesting Organization **MUST NOT** use or retain, without obtaining proper consent, the Subject-Specific Personal Information (received through the Digital Identity Ecosystem) for purposes other than that specified through the Notice and Consent Processor at the time of					Typically it's easier to audit when it's a MUST statement compared to MUST NOT – would consider revising to MUST obtain proper consent on the use or retention of… etc.	The Requesting Organization **MUST** obtain proper consent on the use or retention of the Subject-Specific Personal Information (received through the Digital Identity Ecosystem)	Accepted as Noted	yes
9	The Notice and Consent Processor **MUST** have internal policies and other documentation for limiting use, disclosure, and retention of Personal Information.					"internal policies and other documentation" seems a bit vague as to the level of depth required for these documents, however, can leave to judgment of assessor and doesn't necessarily mean that it's not auditable	No change	Accepted	yes
10	The Notice and Consent Processor **MUST** document the use of the Subject-Specific Personal Information for the purpose of providing notices and obtaining consents within the Digital Identity Ecosystem. Ideally, the Notice and Consent Processor would not have visibility of Personal Information. However, this is dependent on both the implementation and the requirements to present the Subject-Specific Personal Information itself as part of the consent process.					The "ideally" portion could add confusion for this requirement	Replace "Ideally" with "Note: Typically"…	Accepted as Noted	yes

11	The Notice and Consent Processor **MUST** dispose of Personal Information that is no longer required for the digital identity-related purpose for which it was retained.					L12 Organisations must dispose of personal information that is no longer required for the digital identity-related purpose for which it was retained.	Requesting Organizations and Notice and Consent Processors **MUST** dispose of personal information after the retention period expires. See also MANA-2 in the PCTF Notice and Consent component.	Accepted as Noted	Yes, after updates
12	The Network Facilitator **MUST** facilitate the establishment of systems for the sharing of Personal Information.					This feels quite broad/ambiguous – is there any way to be more detailed in what their responsibilities	Align with LIMC-8 The Network Facilitator MUST NOT use, disclose or retain Personal Information beyond that which is required to support their service agreements. For example, acting on their behalf as a service or network provider.	Accepted as Noted	Yes, after updates
13	The Certifying Authority **MUST** define rules for the end-to-end use, disclosure, and retention of Personal Information created as a by-product of the use of the Digital Identity Ecosystem.					New role - Certifying Authority.	Replace "Certifying Authority" with "Governing Body:	Accepted as Noted	Yes
14	The Certifying Authority **MUST** define and implement processes for providing oversight and enforcement of requirements concerning use, disclosure, and retention of Personal Information created as a by-product of the use of the Digital Identity Ecosystem.					New role - Certifying Authority.	Replace "Certifying Authority" with "Governing Body:	Accepted as Noted	Yes
ACCU	**Principle 6 - Accuracy** **Note:** *Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used.*	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**If "No", please recommend adjustment**	**Final Resolution/Next Steps**	**Accepted, Deferred, or Rejected**	**Deemed Auditable**
Process/Function Overview:									
1	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** ensure the process for a User to update inaccurate Personal Information within the Digital Identity Ecosystem exists, and clearly lays out the responsibilities of each party within the Digital Identity Ecosystem including the User's own responsibility.					L7 Consumer identity providers, Third-party data providers and Relying parties must implement policies, procedures, and systems to identify, correct and manage inaccurate or outdated personal information. For Consumer identity providers this may be achieved by providing the Individual with the ability to directly update their personal information at any time.	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** ensure that Users have an ability ~~there is a process~~ ~~procedure for a User~~ to update their inaccurate or outdated Personal Information held by the respective participant of ~~within~~ the Digital Identity Ecosystem ~~exists~~. For example, a consumer-focused identity provider may provide the User with the ability to directly update their Personal Information at any time.	Accepted as Noted	Yes
2	The Disclosing Organization **MUST** implement policies, procedures, and systems to identify, correct and manage (e.g., updating Subject records) outdated Personal Information. An organization will only know that the information is outdated if it asks someone (e.g., the subject for periodic verification), or receives push notifications of updates. Optimal or available options to maintain this information will vary by use case and specific circumstances. Please refer to the Verified Person Profile, especially the ID Maintenance section, for related Conformance Criteria.					See L7 in ACCU 1	Add "inaccurate or outdated" , and add in "Note: Typically" for the explanation part.	Accepted as Noted	Yes
3	The Disclosing Organization **MUST NOT** share Personal Information that is known to be invalid, such as an address where the organization has received returned mail.						Replace "such as" with "For example"	Accepted as Noted	Yes
4	When sharing Subject-Specific Personal Information with a Requesting Organization, the Disclosing Organization **MUST** provide the User with: 1. the ability to review a description or summary of the Subject-Specific Personal Information that is to be shared; and 2. instructions or the means to update such Subject-Specific Personal Information.						No change	Accepted	Yes
5	When sharing Service-Specific Information of a Subject with a Requesting Organization, the Disclosing Organization or Notice and Consent Processor **MAY** provide the User with: 1. the ability to review a description or summary of his/her Service-Specific Information that is to be shared; and 2. instructions or the means to update such Service-Specific Information.						No change. Definition of Service-Specific information is in the Privacy Overview document.	Accepted	Yes
6	To verify the accuracy of the Personal Information received from the Disclosing Organization, the Requesting Organization **SHOULD** provide the User the ability to review a summary or description of the information disclosed.						No change	Accepted	Yes
7	Where the Personal Information obtained from the Digital Identity Ecosystem conflicts with Personal Information that the Requesting Organization holds, the Requesting Organization **MUST** resolve this within its own operation.					Refine wording.	Where the Personal Information that is obtained from other participants of the Digital Identity Ecosystem conflicts with Personal Information that is held by the Requesting Organization ~~holds~~, the Requesting Organization **MUST** have a procedure to resolve the discrepancy ~~resolve this within its own operation~~.	Accepted as Noted	Yes
8	The Notice and Consent Processor **MUST** store an audit trail of notice and consent information. The integrity of this audit trail must be maintained. The retention period for the audit trail will be determined by the governance framework and applicable legislation and regulation.						Clarification: The Notice and Consent Processor **MUST** store an audit trail of notices presented and consent decisions collected/received. ~~notice and consent information.~~	Accepted as Noted	Yes

9	The Governing Body **MUST** define and place rules around how the accuracy of Personal Information can be supported by the Digital Identity Ecosystem. This may include, for example, services that allow (with the Subject's consent) broadcast of updates to subscribed Requesting Organizations.					Minor updates for clarity.	The Governing Body **MUST** define policy and guidance for ensuring ~~and place rules around how the~~ accuracy of Personal Information ~~can be supported by~~ within the Digital Identity Ecosystem. ~~This may include,~~ For example, this may include	Accepted as Noted	Yes
Reference	**Conformance Criteria**	**Level of Assurance (LOA)**							
SAFE	**Principle 7 - Safeguards** **Note:** *Personal information must be protected by appropriate security relative to the sensitivity of the information.*	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**If "No", please recommend adjustment**	**Final Resolution/Next Steps**	**Accepted, Deferred, or Rejected**	**Deemed Auditable**
Process/Function Overview:									
1	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** ensure security measures to protect Personal Information are in place and communicated to the User (as appropriate), and that protections are in place in the event something goes wrong.					Separate out out defining and communicating security measures, and implementing them S1 Organisations must have security policies, processes, controls and measures in place to protect all personal information against loss, theft, unauthorized access, disclosure, copying, use or modification.	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** have ~~ensure~~ security policies, processes, controls and measures in place to protect Personal Information ~~are in place~~ and are communicated to the User (as appropriate), ~~and that protections are in place in the event something goes wrong.~~	Accepted as Noted	Yes
New 1 b						S4 (new) Organisations must implement policies, processes and controls to identify, manage and mitigate incidents and breaches, including reporting externally to other organisations, the regulator, other governing bodies, and / or Individuals, as necessary, appropriate or legally required.	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors MUST implement policies, processes and controls to identify, manage and mitigate security incidents and breaches, including reporting externally to other organizations, regulators, the Governing Body, or Users, as necessary, appropriate or legally required.	Accepted as Noted	Yes
2	The Disclosing Organization **MUST** develop and implement a security policy to protect Personal Information that specifically includes protections employed in the disclosure of the Subject-Specific Personal Information in the context of the digital identity systems concerned.					Reword to be clearer.	The Disclosing Organization **MUST** develop and implement a security policy ~~to protect Personal Information~~ that specifically includes protections applied ~~employed~~ when disclosing ~~in the disclosure of the~~ Subject-Specific Personal Information in the context of the ~~digital identity systems concerned~~ Digital Identity Ecosystem.	Accepted as Noted	Yes
3	The Disclosing Organization **MUST** implement appropriate security safeguards, in accordance with the risks of harm identified in risk assessment (threat risk assessment and/or privacy impact assessment as appropriate), to protect access to Personal Information, both at rest and in transit.					S2 Security safeguards must be appropriate to the risk of harm and the sensitivity of personal information identified in risk assessment (threat risk assessment and / or privacy impact assessment as appropriate).	The Disclosing Organization and Requesting Organization **MUST** implement ~~appropriate~~ security safeguards, ~~in accordance~~ appropriate to ~~with~~ the risk of harm and sensitivity of Personal Information identified in risk assessment (threat risk assessment and/or privacy impact assessment as appropriate), to protect access to Personal Information ~~both at rest and in transit~~.	Accepted as Noted	Yes
4	The Disclosing Organization **MUST** employ security safeguards, in accordance with the risks of harm identified in risk assessment (threat risk assessment and/or privacy impact assessment as appropriate), appropriate to the sensitivity of Personal Information to the Subject and as well as to the risk of fraud or abuse.					Separate out the at rest and in transit as separate criteria.	The Disclosing Orgnization and Requesting Organization **MUST** implement ~~appropriate~~ security safeguards to protect ~~access to~~ Personal Information~~,~~ both at rest and in transit.	Accepted as Noted	Yes
5	The Disclosing Organization **MUST** conduct a regular review and update of security measures relating to the Digital Identity Ecosystem.					S5 Organisations must regularly review and update security measures relating to the digital identity ecosystem. Combine into single criteria for multiple roles.	The Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, and Network Facilitators **MUST** conduct a regular review and update of their security measures relating to the Digital Identity Ecosystem.	Accepted as Noted	Yes
6	The Requesting Organization **MUST** develop and implement a security policy to protect Personal Information that specifically includes protections employed in the receipt of Personal Information in the context of the digital identity systems concerned.					Reword to be clearer.	The Requesting Organization **MUST** develop and implement a security policy ~~to protect Personal Information~~ that specifically includes protections ~~employed~~ applied ~~in the receipt~~ when receiving ~~of~~ Personal Information in the context of the Ddigital Eidentity Ecosystem~~s concerned~~.	Accepted as Noted	Yes
7	The Requesting Organization **MUST** implement appropriate security safeguards to protect access to Personal Information, both at rest and in transit.						Remove. Merged as part of updated SAFE-4.	Accepted as Noted	N/A
8	The Requesting Organization **MUST** employ security safeguards appropriate to the sensitivity of Personal Information to the Subject and as well as to the risk of fraud or abuse.						Remove. Merged with SAFE-3.	Accepted as Noted	N/A
9	The Requesting Organization **MUST** conduct a regular review and update of security measures relating to the Digital Identity Ecosystem.						Remove –merged into SAFE-5	Accepted as Noted	N/A
10	The Notice and Consent Processor **MUST** develop and implement a security policy to protect Personal Information that specifically includes protections employed in the Notice and Consent processes.						Remove. Redundant with SAFE-3 and updated SAFE-11	Accepted as Noted	N/A

11	The Notice and Consent Processor **MUST** implement appropriate security safeguards.					Reword to define what appropriateness means.	The Notice and Consent Processor and Network Facilitator **MUST** implement ~~appropriate~~ security safeguards as specified in relevant criteria the PCTF Infrastructure (Technology and Operations) component.	Accepted as Noted	Yes
12	The Notice and Consent Processor **MUST** employ security safeguards appropriate to the sensitivity of any Personal Information presented to the Subject in the privacy notice as well as to the risk of fraud or abuse.					Reword to match other criteria with similar requirements in SAFE-3	The Notice and Consent Processor **MUST** ~~employ~~ implement security safeguards appropriate to the sensitivity of any Personal Information presented to the Subject in the privacy notice, and to the risk of harm ~~identified in risk assessment~~ (threat risk assessment and/or privacy impact assessment as appropriate), to protect access to Personal Information ~~as well as to the risk of fraud or abuse.~~	Accepted as Noted	Yes
13	The Notice and Consent Processor **MUST** conduct a regular review and update of security measures relating to the Digital Identity Ecosystem.						Remove –merged into SAFE-5	Accepted as Noted	N/A
14	The Network Facilitator **MUST** develop and implement a security policy appropriate to the function of the network. This will normally involve ensuring that the Network Facilitator minimizes its visibility of Personal Information.					Minor updates for clarity.	The Network Facilitator **MUST** develop and implement a security policy appropriate to the function of the network. Note: Typically this will ~~normally~~ involve ensuring that the Network Facilitator minimizes its visibility of Personal Information.	Accepted as Noted	Yes
15	The Network Facilitator **MUST** implement appropriate security safeguards.					Reword to define what appropriateness means.	REMOVE - merge with SAFE-11	Accepted as Noted	N/A
16	The Network Facilitator **MUST** conduct a regular review and update of security measures relating to the Digital Identity Ecosystem.						REMOVE– merged into SAFE-5	Accepted as Noted	N/A
17	The Governing Body **MUST** implement governance arrangements to include minimum security standards, assessment of participant security arrangements (where appropriate) and placing contractual obligations on participants to meet minimum security standards.					Minor updates for clarity.	The Governing Body **MUST** define and implement governance arrangements …	Accepted as Noted	Yes
18	Digital Identity Ecosystem Participants **MUST** perform a risk assessment (threat risk assessment and/or privacy impact assessment as appropriate) in order to ascertain the risks associated with their processing of Personal Information.						No change	Accepted	Yes
Reference	**Conformance Criteria**	**Level of Assurance (LOA)**							
OPEN	**Principle 8 - Openness** **Note:** *An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.*	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**If "No", please recommend adjustment**	**Final Resolution/Next Steps**	**Accepted, Deferred, or Rejected**	**Deemed Auditable**
Process/Function Overview:									
1	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** ensure the Subject is able to readily obtain clear and understandable information concerning the Digital Identity Ecosystem, how the Subject's privacy is protected, where to go for more information and who to contact for help.					T1 Organisations must be transparent about their identity-related data collection and use practices, products and services. T2 Consumer identity providers and Relying parties must inform Individuals of the following in easy-to-understand language. This information must be easily available and accessible: …	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors MUST ensure the Subject is able to readily obtain clear and understandable information concerning • the Digital Identity Ecosystem (which may reference information maintained by the Governing Body), •what personal information is collected, used, retained or disclosed, •the purposes for the collection, use, retention or disclosure, •the names or categories of third-party recipients of personal information, •an explanation of the Subjects's privacy rights and how to exercise them, •how the Subject's personal information is protected, •where to go for more information, and •who to contact for help.	Accepted as Noted	Yes, after updates
2	Disclosing Organizations, Requesting Organizations, and Notice and Consent Processors **MUST** provide help and guidance when a User makes an access request pertaining to a different part of the Digital Identity Ecosystem. This may involve having the User identify the Requesting Organization through activity history, a consent receipt, and/or engaging the Network Facilitator or Governing Body to support identification of the relevant participant.					Minor update for auditability.	Disclosing Organizations, Requesting Organizations, and Notice and Consent Processors **MUST** have a process to…	Accepted as Noted	Yes
3	The Disclosing Organization **MUST** provide information to Users concerning the Disclosing Organization's role following the Governing Body guidelines.					Combine criteria that apply to multiple roles.	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, and Network Facilitators **MUST** have a process to provide information to Users concerning ~~the~~ their role in the Digital Identity Ecosystem following the Governing Body guidelines, when requested.	Accepted as Noted	Yes

4	The Disclosing Organization **MUST** ensure information concerning the Disclosing Organization's role is clearly delineated from other services and functions provided by the organization (that are not part of the Digital Identity Ecosystem per se).					Can this be combined with OPEN-3. For now, leave separate.	Disclosing Organizations Requesting Organizations, Notice and Consent Processors, and Network Facilitators **MUST** ensure information concerning ~~the Disclosing Organization's~~ their role is clearly delineated from other services and functions provided by the organization (that are not part of the Digital Identity Ecosystem per se), such as marketing.	Accepted as Noted	Yes
5	The Requesting Organization **MUST** provide information to Users concerning the Requesting Organization's role following the Governing Body guidelines.						Remove. Merged into OPEN-3.	Accepted as Noted	N/A
6	The Requesting Organization **MUST** ensure information concerning the Requesting Organization's role is clearly delineated from other services and functions provided by the organization (that are not part of the Digital Identity Ecosystem per se).						Remove. Merged into OPEN-4.	Accepted as Noted	N/A
7	The Notice and Consent Processor **MUST** provide information to Users concerning the Notice and Consent Processor's role following the Governing Body guidelines.						Remove. Merged into OPEN-3.	Accepted as Noted	N/A
8	The Notice and Consent Processor **MUST** ensure information concerning the Notice and Consent Processor's role is clearly delineated from other services and functions provided by the organization (that are not part of the Digital Identity Ecosystem per se).						Remove. Merged into OPEN-4.	Accepted as Noted	N/A
9	The Network Facilitator **MUST** provide information to Users concerning the Network Facilitator's role following the Governing Body guidelines.						Remove. Merged into OPEN-3.	Accepted as Noted	N/A
10	The Network Facilitator **MUST** ensure information concerning the Network Facilitator's role is clearly delineated from other services and functions provided by the organization (that are not part of the Digital Identity Ecosystem per se).						Remove. Merged into OPEN-4.	Accepted as Noted	N/A
11	The Governing Body **MUST** ensure that the policies and practices for the management of Personal Information by the Digital Identity Ecosystem are clear, consistent and complete.					To be auditable, make it a clearer responsibility of what Governing Body must do.	The Governing Body **MUST** develop and maintain clear and understandable information about how, in general terms, personal information is collected, used and disclosed within the Digital Identity Ecosystem and how Users can exercise their privacy rights.	Accepted as Noted	Yes, after updates
12	The Governing Body **MUST** work with the ecosystem's participants to ensure the privacy policy and practices information required by Openness 8 criteria is presented in a consistent manner to avoid conflicting or confusing messages.					Is this redudandant with other criteria.	No leave in, as this is the review aspect not covered by other criteria. Add "have a procedure to"	Rejected	Yes
13	The Governing Body **MUST** provide guidelines to all participants on compliance with the requirements statements noted above in this section, and review conformance by the participants to ensure they follow the guidelines.					Reword to be clearer. Last clause can be removed, it is covered by AC	The Governing Body **MUST** provide guidelines to all participants on compliance with the criteria ~~requirements~~ statements ~~noted above~~ in this Principle 8 - Openness section, ~~and review conformance by the participants to ensure they follow the guidelines.~~	Accepted as Noted	Yes, after updates
14	The Governing Body **MUST** ensure that there are processes in place to respond to a User's request for information.						The Governing Body **MUST** ~~ensure~~ verify that each Participant, including the Governing Body, ~~are~~ has processes in place to respond to a User's request for information.	Accepted as Noted	Yes
Reference	**Conformance Criteria**	**Level of Assurance (LOA)**							
INDI	**Principle 9 - Individual Access** **Note:** *Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.*	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**If "No", please recommend adjustment**	**Final Resolution/Next Steps**	**Accepted, Deferred, or Rejected**	**Deemed Auditable**
Process/Function Overview:									
1a						New	Participants in the Digital Identity Ecosystem **MUST** have appropriate policies concerning the existence, use, and disclosure of Personal Information.	Accepted as Noted	Yes, after updates
1b						R1 Organisations must have appropriate policies and processes in place to manage complaints and rights requests from Individuals. R4 Organisations must make sure they train applicable staff to be able to respond to any requests or complaints.	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **SHOULD** have appropriate processes to manage complaints and rights-requests from Users including: - clearly setting out the responsibilities of other entities involved for resolution - training applicable staff to be able to respond to any requests or complaints	Accepted as Noted	Yes, after updates

1	Participants in the Digital Identity Ecosystems will often provide inbuilt features that automatically provide the User with information concerning the existence, use, and disclosure of their Personal Information within the Digital Identity Ecosystem. Where such features exist, Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** ensure the principle of individual access (as described in PIPEDA) is met. When participants in the Digital Identity Ecosystem do not provide inbuilt features providing the User with information concerning the existence, use, and disclosure of their Personal Information, then the process for obtaining such information **MUST** be clear, straightforward and in-line with PIPEDA or other relevant legislation.					Separate into two criteria for clarity. R2 Organisations should aim to provide inbuilt features that automatically provide the Individual with the ability to access and correct their personal information.	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **SHOULD** provide inbuilt features that automatically provide the User with the ability to access and correct their personal information. Note: Because the Notice and Consent Processor facilitates the sharing of, but does not use, Personal Information, the "individual access" is likely to be limited to viewing the audit trail of Notice and Consent activities relating to the Subject.	Accepted as Noted	Yes, after updates
2	The Disclosing Organization **MUST** provide clear means for the User to obtain information concerning the existence, use and disclosure of their Personal Information as it pertains to handling of the information within the context of the Digital Identity Ecosystem.					R3 Where organisations do not provide inbuilt features allowing the Individual to access and correct their personal information, they must create a process to do so and make this clear to Individuals. This includes clearly setting out the responsibilities of other organisations involved, where relevant. R5, R6, R7, R8	Where Disclosing Organizations, Requesting Organizations and Notice and Consent Processors do not provide inbuilt features, they **MUST** create a process for Users to obtain information concerning the existence, use and disclosure of their Personal Information, and make this clear to Users	Accepted as Noted	Yes, after updates
3	The Requesting Organization **MUST** provide clear means for the User to obtain information concerning the existence and use of their Personal Information received via the Digital Identity Ecosystem.						REMOVE - Combined into #2.	Accepted as Noted	N/A
4	If the Requesting Organization determines that the Personal Information it receives from the Digital Identity Ecosystem is inaccurate or incomplete, processes **MAY** exist to notify the relevant Disclosing Organization of the problem.						Change to SHOULD to be auditable.	Accepted as Noted	Yes, after updates
5	The Notice and Consent Processor **MUST** provide clear means for the User to obtain information concerning the existence, use, and disclosure of their Personal Information within the Notice and Consent Processor. Because the Notice and Consent Processor exists to facilitate the sharing of Personal Information but then does not subsequently use the Personal Information, the "individual access" is likely to be limited to viewing the audit trail of Notice and Consent activities relating to the Subject.						REMOVE - Combined with #1 and #2		N/A
6	The Network Facilitator **SHOULD NOT** have access to Personal Information (other than potentially anonymous identifiers that the Network cannot link back to Subjects). If the Network Facilitator does have access to Personal Information, then the Network Facilitator **MUST** comply with the PIPEDA "Individual Access" principle.						Remove the repetetive verbiage: The Network Facilitator SHOULD NOT have access to Personal Information (other than potentially anonymous identifiers that the Network cannot link back to Subjects). If the Network Facilitator does have access to Personal Information, then they MUST comply with INDI 1 and 2	Accepted as Noted	Yes, after updates
7	The Governing Body governance arrangements **MUST** ensure that "Individual Access" processes and guidelines are provided and appropriate to the information exchanged through the Digital Identity Ecosystem.						Replace "ensure that" with "include a section on"	Accepted as Noted	Yes, after updates
Reference	**Conformance Criteria**	**Level of Assurance (LOA)**							
CHAL	**Principle 10 - Challenging Compliance** **Note:** *An individual shall be able to challenge an organization's compliance with the above principles. Their challenge should be addressed to the person accountable for the organization's compliance with PIPEDA, usually their Chief Privacy Officer.*	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**If "No", please recommend adjustment**	**Final Resolution/Next Steps**	**Accepted, Deferred, or Rejected**	**Deemed Auditable**
Process/Function Overview:									
1	The name or title, and contact information, of the person responsible for compliance in the Disclosing Organization, Requesting Organization and Notice and Consent Processor, and means to engage in recourse against them, **MUST** be made simple and available.					Minor updates for clarity.	**...MUST** be clearly available for anyone requesting it. ~~made simple and available.~~	Accepted as Noted	Yes
2	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, and Network Facilitators each **MUST** have a compliance management program that: - clearly and simply differentiates involvement in the Digital Identity Ecosystem from the organization's other activities; and - assists the User in obtaining the support required, even if the complaint needs to be directed to another participant in the Digital Identity Ecosystem.						No change	Accepted	Yes
3	The Governing Body **MUST** put in place processes to triage and direct complaints in order that the Subject is provided with the necessary support from the correct participant, as efficiently and clearly as possible.					Minor updates for clarity. Add in timeliness and recording actinosn from CHAL-4.	The Governing Body **MUST** provide guidance to Participants ~~put in place for handling processes to triage and direct~~ on how to notify and respond to complaints in a **timely manner as well as record actions** in order that the Subject is provided with the necessary support from the correct participant, as efficiently and clearly as possible.	Accepted as Noted	Yes
4	The Governing Body **MUST** include procedures on how to notify and respond to complainants in a timely manner as well as record decisions and actions to ensure consistency with the Privacy Conformance Profile and to protect the participants of the Digital Identity Ecosystem.						Remove - Merged with CHAL-3 by adding timliness and record actions..	Accepted as Noted	N/A

General Feedback	Comment / Resolution
The privacy framework takes an approach that will actually make it very difficult for organisations doing privacy well to satisfy the requirements. In some parts the requirements suggest an approach to digital identity that does not reflect the current market and so would discriminate against those offering digital identity in a different way. Any defined role responsible for providing further guidelines or rules must be careful not to try and make a one-size-fits-all approach and to understand the different business and operating models on the market.	Acknowledged. For this version, adjusted criteria to take a more outcomes-based approach. Future revisions may consider wider range of privacy frameworks.
The other main issue is the lack of clarity of the different roles described which means some of the requirements do not make sense with regard to the actual roles in the digital identity ecosystem nor do they accommodate the fact that one organisation may have multiple roles. For example, if a network facilitator is a SaaS provider and hosts data for its clients, a requirement that they should never store or be able to access personal information makes no sense. This scenario can also mean that the end customer is the one with the control over the data, and elements such as its retention and deletion, so requiring such a SaaS provider to collect data or create logs or access records above and beyond what is required to deliver the product or service is not a privacy-friendly approach.	Reworded criteria to better reflect this (e.g. LIMC-8, LIMU-12); the Overview does recognize that a given organization may take on one or more roles.
Some requirements are impossible to comply with such as requiring one entity to provide the user with information to understand the risks posed by an entirely separate entity, which it has no control over nor knowledge about what the other entity does with personal information. Equally, SaaS providers will always need some level of access to the data for troubleshooting, even where encryption is used at rest and in transit.	Acknowledged. Auditbility review and resulting updates may paritally address this. As well reworked governing body criteria that also partially addresses this.
The framework does not seem to accommodate the scenario where the user is in control, has access to their information and initiates activities like data sharing, updating and deleting their information. A privacy-friendly architecture can mean the organisation has no access to the user data. This is how XX organization operates for its B2C digital identity product. This approach means individuals have a way to prove their identity with multiple organisations and the identity provider therefore has no view into what data items have been shared and no way or authority to proactively update relying parties if a user updates or deletes certain information.	Acknowledged. Neither Privacy, nor Notice and Consent, explicitly state that the Discloing Organization could be the Subject/User, yet the definition of that role states the Disclosing Organization can be a person. As well, the Privacy Overview states: "Baseline conformance criteria (See BASE in the Privacy Conformance Profile) do not address use cases where the Subject acts as the Disclosing Organization." The other sections are intended to apply. For next revision, review all criteria for this use case.
The framework therefore risks dictating the technical and operational arrangements of multiple organisations which is inappropriate and discourages innovation.	See previous response.
The other key aspects to take into account when designing an effective privacy framework are that Candian privacy law is undergoing reform and the principles overlap. Any framework needs to accommodate the reforms, in particular as regards the changing approach to consent, rather than rely on what will be old law. The overlap in the principles leads to a lot of repetition or duplication of requirements whereas a more effective approach would be to focus on the desired outcomes. This will also the framework to operate beyond Canada and allow organisations also subject to other privacy laws to be able to satisfy the requirements.	Acknowledged. Recommend that future revisions look at wider range of Privacy frameworks. For this revision, worked on streamlining criteria for overlap and redundancy.
Both Canadian and non-Canadian organisations may be subject to multiple privacy laws and most will operate global compliance programmes to accommodate all the requirements. In some cases this can lead to organisations already going above and beyond Canadian law compliance for all individuals, such as offering Canadians the range of rights found in the EU's GDPR not just those in PIPEDA. It also means organisations may have to design their compliance efforts in a way that achieves the outcomes required in all the relevant jurisdictions, rather than having separate efforts precisely tailored to each specific jurisdiction.	Acknowledged. Recommend that future revisions look at wider range of Privacy frameworks, and how to address multi-jurisdictions.

There is often an assumption that everything is being done on the basis of consent, which is not the case, and should not be the case given that ID checks are a requirement or legal necessity in many cases and an individual simply cannot decide to refuse them and continue with the product or service. Assuming consent is always the right approach undermines and makes meaningless any consent given. It is worth noting that one of several exceptions to consent in the draft new Canadian privacy Bill is that consent is not necessary where the activity is necessary to provide a product or service. Consent also means different things in different privacy laws so an organisation subject to multiple laws cannot at a high level attest to a requirement in this framework that consent is always obtained or obtained in a given way, when this would lead them to breach laws in other jurisdictions. They can though attest that they obtain consent where this is legally required, as their products and services can be built to accommodate jurisdictional differences.	Acknowledged. Recommend this be considered for next revision of both the Privacy, and more specifically, for the Notice and Consent component. Currently, the introduction to the Privacy Profile states: "In the Privacy conformance criteria, the phrase "notice and consent" is to be interpreted as "notice, or notice with consent" recognizing there are use cases where notice is required but explicit consent is not required."
Many of the requirements are about an entity having confidence in the compliance of another entity. However, it is not clear what 'have confidence' means? Does it require due diligence? Contractual obligations? For example, in some jurisdictions diligence and contractual obligations would both be a legal requirement for an organisation engaging an ID provider or service. It needs to be clear what complying with a requirement requires and looks like, otherwise there is wide scope for interpretation and misinterpretation which ultimately undermines the requirement in question.	Auditability review revisited all criteria to replace vague language with more objectve, auditable outcomes.
There are repeated requirements relating to breaches. In many jurisdictions, including Canada, risk assessment and breach notification requirements required by law are on the entity suffering the breach. It would be highly inappropriate for a third party to report another organisation's breach to the regulator. So the requirements for some of the defined entities oversteps their remit and authority, given the role description, and conflicts with the privacy law requirements. This sets organisations up to fail as they will inevitably comply with privacy laws over the framework.	Intention is that criteria are consistent with PIPEDA reporting guidance. Updated Governing Body requirement to "that breaches are reported by participants to relevant privacy regulators and Subjects" Also noted in the Overview: Requirements for more general fraud monitoring, reporting, and actions to be taken within the Digital Identity Ecosystem warrant further consideration and development within the PCTF context.
In a similar vein some of the requirements for Governing Bodies overstep the mark and provide regulator-type powers that may have no basis in law, especially if a governing body is created that is a private-sector organisation. If the Governing Body's role is to check compliance against this framework, then their obligation to just to check the requesting organisation has satisfied the various requirements. Not to pass judgement on whether they agree with how they have done it or not. It is for the privacy regulator to decide on things like excessive data collection and similar.	Updated much of the Governing Body working to "provide guidance" rather than enforce or verify. Also, next major release of PCTF to take holist view of the role of the Governing Body across all components, not only Privacy.
Some requirements are also just statements of fact rather than setting out an actual requirement, and some are vague and opaque, so examples could help explain what the requirement is looking for. Many are also very detailed but not tailored to digital identity.	Updated. Criteria that are intended as statements, now identified as Notes, not auditable critieria.
Specific comments on particular sections	
BASELNE	**See Privacy criteria tab of this spreadsheet for responses.**
It may not be appropriate for some of the entities involved to provide privacy notices as they may have no interaction with the individual. For example: network facilitators and governing bodies. Also, who provides notice at what point depends on the scenario in question. A disclosing organisation may be acting on behalf of a requesting organisation and so in that scenario it is the requesting organisation who needs to explain to the individual what data they require and why.	
An outcome-focused approach would have a requirement that the organisation the individual is interacting with and / or the one requiring the ID check or ID-related information has the responsibility to provide relevant and appropriate privacy information. Organisations whose role is to provide a back-end ID-related service of some kind will have no direct relationship with the individual, may even be invisible to them, and have no responsibility	
ACCOUNTABILITY	

The first two requirements duplicate each other. It is not necessary to name a specific individual responsible for privacy. Organisations may have more than one person in a privacy team, and a general contact is better (such as privacy@company.com) as it doesn't need updating every time the person changes role or leaves the company. Depending on the query, it may be different people who are involved or responsible for responding, or it may be a team effort.

An outcome-focused approach would have a requirement that the organisations need to provide the user with a clear means to easily contact the organisation on privacy matters.

It is also unecessary to require a PIA just for disclosure aspects of digital identity. Depending on the setup a disclosing organisation may need a PIA for some or all aspects of the parts they are responsible for. They may not be in a position to map the entire ecosystem, given they have no involvement in many aspects of it.

An outcome-focused approach would have a requirement that a PIA is required where either the applicable privacy law requires it or where the activity carried out by the disclosing organisation presents high privacy risks to Users. This would be a more proportionate approach that accommodates many different business models.

IDENTIFYING PURPOSES

Requirements in this section are over-complicating matters for all the entities involved. An outcome-focused approach would have requirements that the entity wanting personal information needs to have a clear purpose for doing so, and must communicate that to the individual whose information they are asking for.

A suggested outcome-focused approach that aligns with Canadian privacy law

The PIPEDA principles overlap which often means elements of an organisation's compliance efforts satisfy multiple principles at the same time. It also means an organisation attesting to compliance by listing each principle individuall ends up with duplication and repetition instead of a coherent view of where they stand.

The principles can be reframed as the following required outcomes, which also take account of the upcoming reform and allow the framework to be complied with by organisations also subject to privacy laws in other jurisdictions.

● Accountability: each organisation involved in the activity should be clear on their obligations and responsibilities, needs to comply with the principles, and be accountable for it.
● Limitations: organisations collecting personal information from individuals need a clear, defined, justifiable purpose for doing so, and can only collect the minimum information required to fulfill this purpose. Any collection must be fair and lawful and information must be as accurate, complete, and up-to-date as possible. Organisations can then only use, keep and disclose the information for this purpose.
● Transparency: organisations need to tell individuals about their information collection and use practices, including what they are collecting and why, who they will share it with, and any risks or consequences.
● Consent: organisations may need consent to collect the personal information, or to use, keep or disclose it beyond the identified purpose. Organisations should offer choices for information not necessary for the product or service.
● Individual rights: organisations must be able to provide and facilitate the rights (access, correction and any others introduced in law) and provide complaint, investigation and recourse mechanisms.
● Security: organisations must protect personal information in a way that is appropriate to how sensitive it is, and protect all information against loss, theft, unauthorised access, disclosure, copying, use or modification.

Suggested privacy framework

Roles in the digital identity ecosystem

● Consumer identity provider - an organisation providing individuals with a digital identity in one form or another. Thi could be an identity card, a digital app or wallet of attributes, a set of credentials, and so on.

● Business identity provider - an organisation providing other businesses with identity verification products and services so the business can carry out checks on their own customers / end users.

● Relying party - an organisation that requires an individual to prove their ID.

● Third-party data provider - an organisation holding identity information that can be accessed or sold to Identity providers or Relying parties to enable, complete or enhance an ID check. This could be a government database, the issuing authority of an ID document, a data broker, a credit reference agency and so on.

● Third-party service - an organisation that interacts with personal information but is providing a non-data service, such as a datacentre, software or technology tools, a consent manager tool and so on.

● Individual - the person who the identity information is about, who obtains or creates some kind of digital identity, and who is asked to prove their identity by a relying party.

● Governing body: an organisation with the authority to assess and / or enforce compliance with relevant legislation, guidance and this framework.They may also issue guidance and best practices. (This will usually be an official regulator but there may be other organisations tasked with some of these activities, such as producing and assessing compliance with guidance.

Accountability

A1 Each organisation must have in place an appropriate privacy management programme that includes policies, practices and procedures to comply with applicable privacy laws, including but not limited to the following.
● What information they collect, use, keep and disclose and why.
● Privacy risk assessment.
● Individual rights, complaints and questions.
● Any relevant restrictions on collection, use, retention or disclosure (legal, contractual).
● Training and awareness.
● Diligence on third parties (includes customer, suppliers, service providers, partners).
● Security measures and incident response and management.

A2 Each organisation must have one or more people who are responsible and have authority for privacy matters and publicly-available contact details to reach those people.

A3 Organisations must make sure they have trained relevant staff appropriately to be able to respond to privacy-related requests, complaints and queries.

A4 Each organisation has to set out their role in the digital identity ecosystem and to agree in writing between the relevant organisations who has what responsibilities with regards to user personal information. This must cover:
● whether consent is required and any requirements for the form and manner of the consent;
● restrictions on use and disclosure;
● data sharing;
● user rights;
● transparency obligations;
● consent obligations if appropriate;
● security obligations; and
● data deletion arrangements.

A5 The Governing body must:
● have clear terms of reference with regard to its role and remit including but not limited to:
○ receiving complaints about an organisation’s compliance with this framework;
○ assessing and enforcing compliance with this framework;
○ receiving complaints about an organisation’s compliance with relevant legislation or regulator guidance;
○ assessing and enforcing compliance with relevant legislation or regulator guidance; ○ produce appropriate guidance.
● not take on the role, remit or tasks of another governing body.

Limitations

L1 Organisations collecting personal information from individuals need a clear, defined, justifiable identity-related purpose for doing so.

L2 Business identity providers and third-party data providers must do appropriate diligence to make sure that Relying parties have a clear, defined, justifiable identity-related purpose.

L3 Organisations collecting personal information from individuals can only collect the minimum information required t fulfill the stated identity-related purpose(s).

L4 Organisations disclosing personal information must only disclose the minimum necessary for the identity-related purpose(s) and comply with any regulatory rules or relevant policies relating to masking.

L5 Organisations collecting personal information from individuals must make sure the collection is fair and lawful and they do not deceive or mislead individuals.

L6 Personal information collected, held, used or disclosed must be as accurate, complete, and as up-to-date as possible.

L7 Consumer identity providers, Third-party data providers and Relying parties must implement policies, procedures, and systems to identify, correct and manage inaccurate or outdated personal information. For Consumer identity providers this may be achieved by providing the Individual with the ability to directly update their personal information at any time.

L8 Third-party data providers and Business identity providers must not disclose personal information that they know to be invalid.

L9 Organisations who become aware that personal information they hold or receive is inaccurate may make arrangements to inform other relevant organisations of this.

L10 Organisations can only use, keep and disclose the personal information for identity-related purpose(s). They cannot use that identity information for other unrelated purposes, such as marketing.

L11 Organisations must have a retention schedule in place. Consumer identity providers should allow Individuals to decide how long they keep their card, account, wallet and so on. Business identity providers and Third-party data providers should set default retention periods, pass on any regulatory retention requirements to Relying parties and allow Relying parties to determine retention for the information relating to Individuals they are ID checking through th providers. Business identity providers and Third-party data providers must facilitate the Relying party determining their own retention for their own data.

L12 Organisations must dispose of personal information that is no longer required for the digital identity-related purpose for which it was retained.

Transparency

T1 Organisations must be transparent about their identity-related data collection and use practices, products and services.

T2 Consumer identity providers and Relying parties must inform Individuals of the following in easy-to-understand language. This information must be easily available and accessible.

● What personal information is collected, used, retained or disclosed.

● The purposes for the collection, use, retention and disclosure.

● Who data is disclosed to or shared with and why.

● Contact details for privacy matters.

● The access, correction and complaint rights (and any other rights that may apply).

● How to make access and correction or other requests, and how to complain.

● Security measures in place.

● Any relevant risks or consequences.

● Any information or documents to explain the organisation's policies, practices or processes.

T3 Business identity providers, where possible and appropriate, should include in products and services the ability for Relying parties using those products and services to provide relevant privacy information to Individuals.

Consent

C1 Organisations in the digital identity ecosystem must be clear about when consent from Individuals is required (legally or contractually) and must communicate this to other relevant organisations involved along with any requirements on the form and manner of the consent.

C2 Organisations requiring consent must define whether a consent is for a one-time or ongoing use or disclosure.

C3 Organisations requiring consent must define whether and in what circumstances a consent can be revoked and any consequences of this revocation.

C4 Organisations must be clear about, and inform the Individual as appropriate of:

● whether they are collecting consent for themselves or on behalf or another organisation, or

● whether the consent is for one time or ongoing; and

● whether and in what circumstances a consent can be revoked and any consequences of this revocation

C5 Organisations responsible for collecting a consent (as identified in A4) must make sure the information provided for that consent is clear, understandable and meaningful to the Individual. Relevant organisations may need to co-operate on this where one is acting on behalf of the other.

C5 Organisations responsible for getting consent (as identified in A4) must record that consent in some way.

C6 Organisations collecting a consent on behalf of another organisation must provide or make it available to that other organisation.

C7 For arrangements where an Individual's consent covers multiple, future uses or disclosures, the organisation with that information must make sure that consent has not expired or been revoked before carrying out such uses or making such disclosures.

C8 When an organisation requiring consent is made aware that consent is no longer valid, the organisation must cease further collection, use or disclosure of personal information based on this invalidated consent.

C9 Where an organisation provides a way for Individuals to consent to ongoing collection, use or disclosures they must also allow the Individual to review and manage those consents.

C10 Where an organisation wants to use the personal information for another, non-identity-related purpose, it can only do so with the consent of the Individual (or unless otherwise provided in law).

Rights

R1 Organisations must have appropriate policies and processes in place to manage complaints and rights requests from Individuals.

R2 Organisations should aim to provide inbuilt features that automatically provide the Individual with the ability to access and correct their personal information.

R3 Where organisations do not provide inbuilt features allowing the Individual to access and correct their personal information, they must create a process to do so and make this clear to Individuals. This includes clearly setting out the responsibilities of other organisations involved, where relevant.

R4 Organisations must make sure they train applicable staff to be able to respond to any requests or complaints.

R5 Where an Individual requests the disclosure of personal information, the organisation facilitating that disclosure must allow the Individual to first review the information to be shared.

R5 Organisations disclosing personal information must provide a way for the Individual to review what has been shared, with whom and when.

R6 Organisations receiving personal information must provide the Individual with a way to review what has been received, from whom and when.

R7 Organisations receiving contact from Individuals relevant to another organisation in the digital identity ecosystem must provide help and guidance to the Individual.

Security

S1 Organisations must have security policies, processes, controls and measures in place to protect all personal information against loss, theft, unauthorised access, disclosure, copying, use or modification.

S2 Security safeguards must be appropriate to the risk of harm and the sensitivity of personal information identified in risk assessment (threat risk assessment and / or privacy impact assessment as appropriate).

S3 Security safeguards must protect personal information both at rest and in transit.

S4 Organisations must implement policies, processes and controls to identify, manage and mitigate incidents and breaches, including reporting externally to other organisations, the regulator, other governing bodies, and / or Individuals, as necessary, appropriate or legally required.

S5 Organisations must regularly review and update security measures relating to the digital identity ecosystem.

S6 Organisation must make sure they have trained staff on the importance of maintaining the security and confidentiality of personal information, and hold regular staff training on security.