# Assessment Evidence: Consent

* COWI.01 to COWI.05 are PSP PCTF only
* The remaining criteria are part of CAN/CIOSC 103-1

| **ID** | **Qualifier(s)** | ***Conformance Criteria***  **Evidence** |
| --- | --- | --- |
| **COWI** |  | **Consent Wide** General requirements for consent domain atomic processes |
| **COWI.01** | GEN | The entity under assessment MUST have a comprehensive Privacy Policy that:  ● provides a full description of its personal information handling practices;  ● is easily accessible, simple to read, and updated as required; and  ● is made available to clients and disseminated to internal personnel. |
| **COWI.02** | GEN | The entity under assessment MUST periodically audit or review their personal information management practices (including its notice and consent management practices) to ensure that personal information is being handled in the way described by its Privacy Policy. |
| **COWI.03** | GEN | The entity under assessment MUST have a Privacy Management Program in place to ensure legal compliance including the implementation of privacy policies, practices, controls, and assessment tools. |
| **COWI.04** | GEN | As part of its Privacy Management Program, the entity under assessment MUST have processes to manage personal information breaches, which includes reporting, containment, remediation, and prevention steps. |
| **COWI.05** | GEN | The entity under assessment MUST have a Privacy Officer or similar position in place 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). |
| **NOFO** |  | **Notice Formulation** Notice Formulation is the process of producing a notice statement that describes what personal information is being, or may be, collected; with which parties the personal information is being shared and what type of personal information is being shared (as known at the time of presentation); for what purposes the personal information is being collected, used, or disclosed; the risk of harm and other consequences as a result of the collection, use, or disclosure; how the personal information will be handled and protected; the time period for which the notice statement is applicable; and under whose jurisdiction or authority the notice statement is issued. This process should be carried out in accordance with any requirements of jurisdictional legislation and regulation. |
| **NOFO.01** | GEN | The entity under assessment MUST determine what information is required to be included in the notice statement based on all applicable legal, policy, and contractual requirements. This could include, for example:  ● the personal information about the Subject being requested;  ● the purpose for which the personal information is being requested;  ● the legal authority for collecting the personal information;  ● if applicable, the period of time for which the personal information requested will be stored or used; and  ● whether the request is for a one-time disclosure of the personal information or to allow ongoing disclosure for the same purpose (e.g., to allow the Subject to “broadcast” updates to their personal information, such as change of address).  The entity under assessment MUST ensure that the information to be included in a notice statement is precisely defined. This could include, for example, the specific personal information to be shared and any necessary metadata. |
| **NOFO.02** | GEN | The entity under assessment SHOULD provide the notice statement in writing. |
| **NOFO.03** | GEN | The entity under assessment MUST ensure that the notice statement is formulated in a manner that enables the Subject to reasonably understand how their personal information will be collected, used, and/or disclosed. This includes providing the notice statement in a manner that is intelligible (using clear and plain language), concise, easily visible, and easily accessible.  When it is not practical for the notice statement to include all the details pertaining to the request (e.g., the full terms and conditions, detailed metadata), the entity under assessment SHOULD provide the means to allow the Subject to review those details elsewhere. This MUST not be used as a means to make the notice statement less visible, transparent, or accessible. |
| **NOFO.04** | GEN | If the notice statement includes requests for a consent decison from multiple entities, then the entity under assessment MUST ensure that the notice statement is formulated such that the notice statement can be split up into the parts pertaining to each entity so that each entity only receives the evidence of the consent decision relevant to them. |
| **NOFO.05** | GEN | The entity under assessment MUST ensure that a new notice statement is provided to a Subject when the entity under assessment decides to use or disclose personal information that it has already collected from the Subject for a new purpose (i.e., a purpose that is not consistent with the purpose(s) provided in the original notice statement).  The entity under assessment MUST ensure that the new notice statement:  ● identifies the new purpose(s) and the specific personal information that will be used or disclosed for the new purpose(s);  ● includes other applicable information that may be required; and,  ● requests the Subject’s consent to use or disclose the personal information for the new purpose(s). |
| **NOPR** |  | **Notice Presentation** Notice Presentation is the process of presenting a notice statement to a person. |
| **NOPR.01** | GEN | The entity under assessment MUST present the notice statement to the person providing the consent in a manner that is clear and user friendly. |
| **NOPR.02** | GEN | If the notice statement discloses personal information then, before presenting the notice statement, the entity under assessment MUST verify the identity of the person providing the consent, to confirm that the person providing the consent is the Subject of the personal information, by executing the requirements in identity Verification. |
| **CORQ** |  | **Consent Request** Consent Request is the process of asking a person to agree to provide consent (“Yes”) or decline to provide consent (“No”) based on the contents of a presented notice statement, resulting in either a “yes” or “no” consent decision. |
| **CORQ.01** | GEN | The entity under assessment MUST ensure the person providing the consent is the Subject of the personal information based on the requirements in Identity Verification. |
| **CORQ.02** | GEN | The entity under assessment MUST ensure that the level of identity verification is sufficient for the sensitivity of personal data to be provided. |
| **CORQ.03** | GEN | Before requesting consent from a Subject, the entity under assessment MUST determine whether the Subject can withdraw their consent at a later date or whether legal or contractual restrictions prevent or limit the withdrawal of consent.  Where a Subject has the right to withdraw their consent at a later date, the entity under assessment MUST:  ● inform the Subject of this right (subject to reasonable notice and applicable conditions or restrictions) at the time the consent is requested;  ● inform the Subject of how to exercise this right; and  ● ensure that the process for withdrawing consent is as easy for the Subject as the process for providing consent. |
| **CORQ.04** | GEN | If the Subject’s consent is requested as part of a notice statement which also concerns other matters, then the entity under assessment MUST present the request for consent in a manner that:  ● is clearly distinguishable from the other matters;  ● is in an intelligible and easily accessible form; and  ● uses clear and plain language. |
| **CORQ.05** | GEN | The entity under assessment MUST NOT attempt to obtain consent by providing false or misleading information or by using deceptive or misleading practices. |
| **CORQ.06** | GEN | The entity under assessment MUST ensure that the action required to be taken by the Subject to provide consent is clear and straightforward.  If the Subject is offered a choice within the requested consent (e.g., to share a subset of the requested personal information), then the entity under assessment MUST ensure that the action required to make the choice is clear and straightforward. |
| **CORQ.07** | GEN | The entity under assessment MUST ensure that the consent is specific, informed, and unambiguous. |
| **CORQ.08** | GEN | The entity under assessment MUST have processes in place that enable it to easily demonstrate that a Subject has consented to the collection, use, and/or disclosure of their personal information. |
| **CORG** |  | **Consent Registration** Consent Registration is the process of storing the notice statement and the person’s related consent decision. In addition, information about the person, the version of the notice statement that was presented, the date and time that the notice statement was presented, and, if applicable, the expiration date for the consent decision may be stored. Once the consent information has been stored, a notification on the consent decision made is issued to the relevant parties to the consent decision. |
| **CORG.01** | GEN | The entity under assessment MUST collect and store the following evidence of the consent decision:  ● Sufficient information to identify the person who has given the consent;   ● The date, time, or other contextual information about when and how the consent decision was made;  ● The version of the notice statement provided and the personal information requested;  ● The consent decision which MUST be one of accept or decline, for each consent choice presented; and  ● If applicable, the expiration date/time of the consent decision. |
| **CORG.02** | GEN | The entity under assessment MUST store the evidence of the consent decision uniquely (i.e., store the evidence of the consent decision for each consent given) and immutably, such that any update (including any change to the notice statement presented to the Subject) will result in a new record and therefore past records can be recovered. The entity under assessment MUST ensure that the storage of evidence of consent decisions complies with applicable legislation (e.g., in certain cases, data must be stored in Canada). |
| **CORG.03** | GEN | As per Canadian laws related to official language requirements, the entity under assessment MUST store each language variation of the notice statement. |
| **CORG.04** | GEN | The entity under assessment MUST employ processes and procedures to prevent the loss of notice and consent decision records and to limit the impact of any data security violations, and in accordance with relevant law. |
| **CORG.05** | GEN | The entity under assessment MUST follow privacy-preserving practices when storing records of consent decisions. In this context, privacy-preserving practices refer to methods, approaches, or procedures designed to maintain the privacy of consent decision records. |
| **CORG.06** | GEN | If the entity under assessment provides the evidence of the consent decision to another requesting entity:   ● The entity under assessment SHOULD inform the Subject of the identity of the other entity receiving the evidence of the consent decision;   ● If the notice statement includes requests for a consent decison from multiple entities, the entity under assessment MUST split up the notice statement so that each entity only receives the evidence of the consent decision relevant to them. |
| **CORE** |  | **Consent Review** Consent Review is the process of making the details of a stored consent decision visible to the person who provided the consent. |
| **CORE.01** | GEN | The entity under assessment SHOULD provide Subjects with the ability to review and manage all consent decisions made. The entity under assessment SHOULD ensure that these features are be easy to use and provide an efficient and optimal means for Subjects to manage consent decisions. This could include, for example:  ● the ability to review the consent decisions provided to a particular entity; and  ● search facilities so that consent decisions can be easily found. |
| **CORN** |  | **Consent Renewal** Consent Renewal is the process of extending the validity period of a “yes” consent decision by means of increasing an expiration date limit. |
| **CORN.01** | GEN | In order to extend the validity period of a “yes” consent decision, the entity under assessment MUST execute the requirements in Notice Formulation, Notice Presentation, Consent Request, and Consent Registration. The entity under assessment MUST store the resulting updated consent decision. |
| **CORN.02** | GEN | The entity under assessment MUST record the following consent renewal information: the effective date of renewal and the initiating party for the renewal. |
| **CORN.03** | GEN | The entity under assessment MUST make available consent renewal information to the Subject and any Verifier. |
| **COEX** |  | **Consent Expiration** Consent Expiration is the process of suspending the validity of a “yes” consent decision as a result of exceeding an expiration date limit. |
| **COEX.01** | GEN | The entity under assessment MUST ensure that a consent decision expires when the expiration date of the consent decision has passed. |
| **COEX.02** | GEN | Unless the collection, use, or disclosure is permitted without consent, the entity under assessment MUST stop collecting, using, or disclosing the personal information specified in the consent decision and MUST inform any entity to whom the the evidence of the consent decision was sent of the expired consent decision. |
| **COEX.03** | GEN | The entity under assessment MUST record the following consent expiry information: the effective date of expiry and the initiating party for the expiry. |
| **COEX.04** | GEN | The entity under assessment MUST make available consent expiry information to the Subject and any Verifier. |
| **CORV** |  | **Consent Revocation** Consent Revocation is the process of suspending the validity of a “yes” consent decision as a result of an explicit withdrawal of consent by the person (i.e., a “yes” consent decision is converted into a “no” consent decision). |
| **CORV.01** | GEN | The entity under assessment MUST revoke a consent decision when either:  ● the Subject withdraws the consent; or  ● the entity under assessment determines that the consent was not legitimate or lawful, for example, if a fraudulent activity, data breach, or unauthorised access is determined. |
| **CORV.02** | GEN | If a Subject notifies the entity under assessment that they wish to withdraw the consent given and there are no legal or contractual restrictions preventing the Subject from withdrawing consent, then the entity under assessment:  ● MUST inform the Subject of the implications of such withdrawal;   ● MUST NOT prohibit the Subject from withdrawing consent; and  ● MUST ensure that the action required to withdraw the consent is clear, explicit, and straightforward. |
| **CORV.03** | GEN | If it is determined that the consent was not legitimate or lawful, then the entity under assessment MUST revoke the consent decision.   The entity under assessment MUST inform the Subject of the revoked consent decision (if appropriate). **Note**: In the case of identity theft where the Subject is compromised it may not be appropriate to inform the Subject of the revoked consent decision. In the interest of protecting identity information from abuse and privacy breaches, revoking consent in such circumstances MUST be done with great care. The entity under assessment MUST ensure that it has processes in place to prevent erroneous or malicious consent revocation. |
| **CORV.04** | GEN | Unless the collection, use, or disclosure is permitted without consent, the entity under assessment MUST stop collecting, using, or disclosing the personal information specified in the consent decision and MUST inform any entity to whom the the evidence of the consent decision was sent of the revoked consent decision. |
| **CORV.05** | GEN | The entity under assessment MUST record the following consent revocation information: the effective date of revocation, the reason for revocation, and the initiating party for the revocation. |
| **CORV.06** | GEN | The entity under assessment MUST make available consent revocation information to the Subject and any Verifier. |
| **SIWI** |  | **Signature Wide** General requirements for signature domain atomic processes |
| **SIWI.01** |  | No conformance criteria exist. |
| **SICR** |  | **Signature Creation** Signature Creation is the process of creating a signature. |
| **SICR.01** | GEN | The entity under assessment MUST ensure that the entity signing the data can be associated with the electronic data being signed. |
| **SICR.02** | GEN | The entity under assessment MUST ensure that it is clear that the entity intended to sign the electronic record. |
| **SICR.03** | GEN | The entity under assessment MUST ensure that the reason or purpose for signing the electronic data is conveyed in some way (this may be evident from the content of the electronic data being signed). |
| **SICR.04** | GEN | The entity under assessment MUST ensure that the data integrity of the signed transaction is maintained over time including the original electronic data being signed, the electronic signature itself, and any supporting information that may be necessary. |
| **SICR.05** | SES | The entity under assessment MUST ensure that the electronic data has been signed by the entity who is identified in, or can be identified through, a digital signature certificate. |
| **SICR.06** | SES | The entity under assessment MUST ensure that specific asymmetric algorithms are used. |
| **SICR.07** | SES | The entity under assessment MUST ensure that the issuing certification authority (CA) is recognized by the Treasury Board of Canada Secretariat. |
| **SICR.08** | SES | The entity under assessment MUST verify that the issuing certification authority (CA) has the capacity to issue digital signature certificates in a secure and reliable manner. |
| **SICH** |  | **Signature Checking** Signature Checking is the process of confirming that the signature is valid. |
| **SICH.01** | GEN | The entity under assessment MUST ensure that the data integrity of the signed transaction is maintained over time including the original electronic data being signed, the electronic signature itself, and any supporting information that may be necessary. |
| **SICH.02** | SES | The entity under assessment MUST ensure that specific asymmetric algorithms are used. |