|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | It is a great honour to CISWG/AdvCIS communities - for the ISO/IEC 27560 to be voted in and started as a work stream.  This completed a long standing action to Address the Biggest Lie on The Internet, where a international standard was needed for notice and consent, so people can see if consent record structure independently of organisations.  For this we give ISO/IEC 29184 our gratitude.  Special thanks: Par Lanera, Rene Lyod, Reubin Binns, Hugo Roy, for starting the drive for this standard. And extra special thanks to the communities leaders that made this possible from the ground up.  Eve Maler  Joni Brennon  Dazza Greenwood – Computaiton Law @ MIT  Mary Hodder  Kaliya Young,  Harshvander J. Pandit,  Georg Philip Krog  Sal D’Agostino  Paul Knowles  Vitor Jesus |  |  |
| Open Consent Group,  AdvCIS  (forrmally Kantara CISWG) | 155 |  |  |  | Unfortunately, the community work group (CISWG) was archived and a great deal of the consent record work is missing from the 27560, and buried in RF Rand IPR license.  **The document elaborates on the example presented in ISO/IEC 29184 Appendix B: “Example of a  Consent Receipt or Consent Record.  ”**  , that this draft of the 27560, **does not** **elaborate on the Consent Receipt**, in fact it is missing most of the consent receipt work, and just has the headings  The editors of 27560 do not represent the CISWG (now AdvCIS) community of work now archived under RF-RAND and presented in these comments under a new OCG RF-RAND  Commenter note: The missing/ignored 27560 inputs not included in the 27560 that is required. Is the bulk of the capture consent information structure defined in laws and represented in legal notice, captured in a receipt. You can see from these documents, that there is no – “Massive Re-Org” as alluded 2017-10-25. In addition, there is 2 years of Legal Ontology work with the W3C DPV CG ( with the German DPA office) also not included in 27560 | Recommend consulting with the expert community for drafting the ISO specifications, and including the bulk of the work (under RF Rand – Not – Non Assert Covenant of ISI –WG)   |  |  |  |  | | --- | --- | --- | --- | | Version | Date | Summary of Substantive Changes | | | MVCR v.01 | 2014-10-01 | [Notice Registry: Provision MVCR v.01](https://kantarainitiative.org/confluence/display/archive/Notice+Registry%3A+Provision+MVCR+v.01) | | | MVCR v0.5 | 2014-10-01 | [Consent Notice Legislation Map and ISTPA Research](https://kantarainitiative.org/confluence/display/archive/MVCR-Spec-+v.06?searchId=7CZ2RDXO7) | | | MVCR v.0.6 | 2015, 01-08 | Specification for Consent Receipt Generator - | | | MVCR v0.7 | 2015-09-03 | [Minimum Viable Consent Receipt v.7](https://kantarainitiative.org/confluence/display/archive/MVCR+V0.7%3A+Kantara+Templated+Editorial?preview=%2F75432251%2F75400193%2FKI-CISWG-Editorial-MVCR-V0_7-20150904.doc) | | | MVCR Design | 2015-09-08 | [Purpose Specification Design](https://kantarainitiative.org/confluence/display/archive/MVCR%3A+Purpose+Specification+Design?searchId=MTD9HLX9D) | | | MVCR Usability |  | 6 Real Consent Workshops at Digital Catapult - and receipt presentation design | | | 1.1.0 DRAFT 1 | 2017-02-28 | Initial v1.1 draft | | | 1.1.0 DRAFT 2 | 2017-07-12 | Sprint 2 draft. | | | 1.1.0 DRAFT 3 | 2017-08-23 | Sprint 3 draft | | | 1.1.0 DRAFT 4 | 2017-10-19 | Roll up of Sprint 4 – Sprint 6 | | | .   |  |  |  | | --- | --- | --- | | 1.1.0 DRAFT 5 | 2017-10-25 | Major reorg of document. | | | | | 1.1.0 DRAFT 6 | 2017-11-17 | Final revisions and updates to the document. | | | 1.1.0 DRAFT 7 | 2017-11-20 | Additional clean-up | | | 1.1.0 DRAFT 8 | 2018-2-15 | Revisions based on comment from public review period. | | | 1.2 | 2020-7-1 | Update to Notice Receipt for 29184 via 27560 input | | |  |
| Open Consent Group,  AdvCIS  (forrmally Kantara CISWG) | 175, 180, 181 |  |  |  | Note: as previous Chair of CISWG, and now Chair of AdvCIS)   1. This document did not use ISO/IEC 29184 as a reference and the majority of the fields have not been referenced with ISO 29184 work, nor most 29100 references not attributed   Recommend using the terms and definitions in the work, with the references stated in the document  **Section 2 Normative References Section 3 Terms & Definitions** | Recommend, reviewing each term, with first ISO/IEC 29100, then ISO/IEC 29184, and combining/review/replace the existing term with the 29100 +29184 Definitions. |  |
| Open Consent Group,  AdvCIS  (forrmally Kantara CISWG) | 189 |  |  |  | For Example, the first term Collection SHALL use, those normative references in the terms.  The notice/consent receipt as an ISO standard should be an international legal notice used by PI Principles to directly control their data. (– as it reflects the localised legal notices in IoT/CCTV signs and Online Privacy Notices for consent. | 3.1 Collection [refer -  ISO/IEC 29100 + 29184 should be used as references]  For example;  To identify what would count as the PII to be listed in the notice, the organization should consult 4.4 of  ISO/IEC 29100:2011  In addition to using generic language such as “Your personal information will be collected,” where appropriate, based on a determination of the impact in the assessment described in 5.3.3, the organization should  provide the list of specific elements of PII that are collected (e.g., “Your name, address, and telephone number will be collected.”) even if it is obvious what the collected information is. ISO/IEC 29184:2020 |  |
| Open Consent Group,  AdvCIS  (forrmally Kantara CISWG) | 11-22 and 211 - 286 |  |  |  | The terms and references were researched over years ,with the consent type, termination, data retention fields purposely not defined until the ISO/IEC 29184 + GDPR came into force, as these impacted these definitions.  The providence and research to the ISTPA, critical to this was the specification of Explicit consent for sensitive, special categories of data, but more importantly consent for the explicit transfer of personal data by the PII Principal.   1. Without ISO/IEC 29184 as the framework extending the legally defined terms and definitions of the Consent receipt Key fields and vocabulary are missing for explicit consent. 2. Key fields and vocabulary are missing for transborder flows for explicit consent 3. A Key element for evidence or compliance is capturing all Privacy stakeholders 4. Privacy Stake Holder transparency is a Key transparency /security required for any consent type to be possible for explicit consent 5. Delegation is required |  |  |
|  | 210 |  |  |  |  | Adopt new fields above |  |
| Open Consent Group,  AdvCIS  (forrmally Kantara CISWG) | 48 |  |  | te | Primary Purpose has been superceded by the use of DPV for purpose specification, | add to references W3C Data Privacy Vocabulary <https://www.w3.org/ns/dpv> |  |
| Open Consent Group,  AdvCIS  (forrmally Kantara CISWG) | 54 |  |  | te | Significant is the -use of the word transaction. As this was discussed at length in the expert communities. Transaction is  to be used    Section 5.3 - Consent Record ~~Transaction~~ Fields    A consent grant interaction is captured, the consent grant can then be used in subsequent transaction, with a personal data use receipt using the Open Notice Schema, | Recommend replace the term transaction throughout the document and make a rule to not use the term unless ts predicated by the term grant for permissioning a service/system |  |
| Open Consent Group,  AdvCIS  (forrmally Kantara CISWG) | 180 |  |  | te | intro comment in line 180 provides the core references for the fields and the update.  The terms and definitions do not refer to ISO /IEC 29100 and 29184, in which it is explicitly stated at - “Line 180 - terms and definitions given in ISO/IEC 29100, ISO/IEC 181 29184, and the following apply”  After a review of the fields, it is clear that the ISO/IEC 29184 Notice content and consent structure control catalogue was not used to reference the terms. | The terms and references do not refer to the stated references. As a result, this required a thorough assessment and review and comment to provide a Kantara Appropriate input for these comments, from our group.  The definitions and terms - need to match these term definitions with the 29184 Notice controls catalogue |  |
|  | 183 |  |  |  | * [Editors’ Note – Check for and remove any terms that ~~already exist in the Normative reference~~ * ~~documents in the next draft]~~   Strongly recommend that the 29100 and 29184 be used. Editor doesn’t seem to understand this is a legally defined standard not a technically standard written for legal standard..  All terms are required to be defined by ISO 29100 and 29184 and applied with 27560 as a conformance profile to audit identity surveillance technologies. | (request editors use required/normative legal terms and definitions) |  |
| Open Consent Group,  AdvCIS  (forrmally Kantara CISWG) | 190 |  |  | te | Should use the ISO 29184 Collection Control definition, as this is important. | The organization shall provide information that allows PII principals to understand what elements are being collected, even where the collection of the particular elements of PII is obvious .{ISO/IEC 29184} |  |
| Open Consent Group,  AdvCIS  (forrmally Kantara CISWG) | 217 |  |  | te | RE: editor’s note disclosure   ~~Note 1 to entry. We note this here because, for a PII Principal, both this ‘use’ and actual ‘disclosure’ may be termed ‘sharing’ information..~~  This was addressed already the Consent Receipt v1.1. and further addressed in the ISO/IEC 29184 Online privacy notice and consent – content and structure controls.  Additional   * The term - Use is not used in a receipt as the purpose of use is a part of the purpose specification. * Sharing is personal sharing * Legally, the terms Disclosure is well defined as a organization disclosing personal data | The editor’s do not have the required expertise (or knowledge of this topic) this issue has been dealt with by the expert community, with CR V1.1. already. |  |
| Open Consent Group,  AdvCIS  (formally Kantara CISWG) | 348 |  |  | te | Elements of a Consent Record, Receipt  An editorial misunderstanding is that it is Legal notice that provides the consent record information structure for a receipt, which is the focus of the 27560.  In most cases throughout the entire document the word record should instead be a receipt. A receipt standard requires an international ISO Standard, (not a consent record.) | Change to Elements of a Consent ~~Record~~, Receipt  (Review all uses of the term record and change to Receipt) |  |
| Open Consent Group,  AdvCIS  (forrmally Kantara CISWG) | 356 |  |  | te | heading: Consent ~~Record Transaction~~ Receipt Interaction Fields  The fields are used to capture the required elements with a notice in a contextual interaction. AKA - A capture of a consent grant interaction. Granting permission to a system to process personal data. | Change Title: to Consent Receipt Interaction Fields  (review entire document and change transaction to interaction) |  |
| Open Consent Group,  AdvCIS  (forrmally Kantara CISWG) | 391 |  |  | te | This should be a consent receipt ID (not a consent record ID) | change to Consent Receipt ID |  |
| Kantara-Notice and Consent Project Team | 202-204 |  |  | te | Again, (very incorrect)  - Editors’ Note: is describing work that is was achieved already in the CR V1.1. at the CISWG.  A receipt was invented through hackathongs where people we hacking using the law.  It has always been a notice and record, from the provider to receiver, which uses standards os as to be independently usable.  Request to Omit- Un/Expert Editorial  ~~The difference between a ‘record’ and a ‘receipt’ is that the former is kept by the PII controller and the latter is a reference to (or a copy of –depends on implementation) the ‘record’ – the ‘receipt’ is supplied to the PII Principal for their own personal recordkeeping].~~  (the intended and primary use of the initial work in this area was to benefit people, not for the benefit of the identity surveillance technology industry) | Update Editors Note: A person can create/request a consent receipt and provide it to a company, for the purpose of exercising privacy rights - in accordance with the captured context. |  |
|  | 402 |  |  |  | Heading~~: Consent Transaction Parties Fields~~  This should be: Privacy Stakeholders Fields \_ this is equivalent to the ‘personal data recipient’ term in the GDPR.  A critical category of information to be defined to capture a receipt interaction. Is to capture all of the Stakeholder identities in order to product/demonstrate a compliant receipt.  These are (besides the PII Principle)  - PII Controller/Joint Controller  - PII Processor and Sub-Processors (missing altogether at the moment)  -Third Party - Delegated Consent (Identified Third Party) | Change to “Privacy Stakeholder” Fields  (recommend putting all privacy stakeholders in this field) |  |
|  | 512 |  |  |  | Heading 5.6 – Consent ~~Record~~ data Structure –  This is actually called the Purpose Specification Data Structure - | Change to Purpose Specification Structure |  |
|  |  |  |  |  | Consent Type Field (Referring to a consent type Labels for Records of Processing  )  (Note: not to be confused with, or used for a definition of the   legal justification for processing personal data)A notice is used to inform people about the use and processing of personal data.  As people have a legal right to know what privacy rights they have, in addition to the reasonable expectation of privacy.   The privacy rights can be explained easily to a PII Principal, relative to consent, and in a consistent manner across legal and technical domains. Similar to how a receipt works today, with standard capture of a transaction, a notice receipt is a capture of a grant interaction. | |  |  |  |  | | --- | --- | --- | --- | | **Consent Type** | **Definition** | **Examples** | **Applicable Privacy Right  (in progress)** | | incomplete information | When there are not enough information elements for a notice to provide a consent type. | N/A | N/A | | Consent Not Needed | Indicates that there is another legal justification besides consent, expressed consent, explicit consent, being utilised to process personal data | These justifications include; contractual necessity, compliance with legal obligations, protect vital interest of PII Principle, public interest, and the legitimate interests of PII Controller | RIght to processing information Right to Object to processing Etc. | | Implicit Consent | Consent is implicit in the action of PII Principle, in context, not to a prior (implied) action. | Walking into a video surveillance area, past a sign at the entrance to vs zone, - implicit action of walking into surveillance zone - implies consent to the Notice (and governance framework behind the notice) |  | | Implied Consent | implied - implies that - a previous notice (and share understanding) exists - where a opt-in is provided with a short contextual notice (or a notification) - referencing an implied previous notice and shared understanding | Cookie consent |  | | (Notice &) Consent | The captured state of consent record information structure in a receipt vs, Privacy as Expected (PaE),  if it is defined in GDPRas state in which, consent provided was - Freely given, specific and informed unambiguous agreement to processing .. |  |  | | 4. Explicit Consent  (in progress) | undefined CR V1.1 profile of legal elements - like meaningful, knowledgeable, informed, which required additional semantic information structure |  |  | | 5. Consent Directive | The Person defines the privacy requirements of the consent in a Privacy Agreement, where the individual understands and is aware, because the person set the terms. The consent still needs to conform to the legal requirements of Explicit Consent  a consent in which the agreement for the grant of permission, granted by a consent is defined by the PII Principle |  |  | |  |
|  |  |  |  |  | Purpose Category ( the field name) or PII Category the ISO term  Significant input is the PII Categories, updating the PII Category appendix for all implementations.  This set of PII Categories is shared between legal and technical domains, and specification communities. , recommend. | https://lh4.googleusercontent.com/mHCiCIMDDsnn-BwslVP73odi_FSB-clZqQWcqC_N4N6qDwxe0kIEHvqSD2jIzUYYsrJnf5oz56NYUmma5U2zroDDxIomfbcurIMpS5tyBwuncEW8hCGDwgifwKV2kpAYtL8QeMkD  Full [tables can be found at AdvCIS](https://openconsent.atlassian.net/wiki/spaces/IHD/pages/1364918273/Personal+PII+Data+Controller+Categories) |  |
|  |  |  |  |  | Missing Explicit Consent Fields : Required for PII principles to use explicit consent to control data transfer personally.   |  | | --- | | Transboarder Field Considerations | | Third Party Role | | International transfer | | International transfer locations | | International transfer safeguards | | Profiling | | Automated decision making | | Processing Categories | | Data Storage location | |  | | Security considerations for TransBorder Processing | | Field Name: | | Providence of PII | | Source: accessed, controlled and processed at source ? (y/n) | | Sensiive or Special Cat of Data | | Benefitial Owner of PII | |  | |  | | **Explicit Consent** | | Field Name | | informed consent | | knowledgable consent | | meaningful consent | | processing interval and frequency | |  | |  | |  | | **Delegation** | | Field Name | | Type of Delegation (Guardiaship) | | Delegation of processing across boarders | | Data Subject is Child | | Given By Delegation | | Delegate Representative | | Delegate Role | | Consent ID | | Validity | | Applicable Rights | |  |  |