



---

# 1 Consent Receipt Specification

2 **Version:** 1.1.0

3 **Document Date:** 2018-02-20

4 **Editors:** Mark Lizar, David Turner

5 **Contributors:** Richard Beaumont, Chris Cooper, Sal D'Agostino,  
6 Rupert Graves, Iain Henderson, Mary Hodder,  
7 Harri Honko, Andrew Hughes, Tom Jones,  
8 Robert Lapes, Oliver Maerz, Eve Maler, Jim Pasquale,  
9 Samuli Tuoriniemi, John Wunderlich

10 **Produced by:** Consent & Information Sharing Work Group

11 **Status:**

12 This document is a Kantara Initiative Technical Specification Recommendation produced by  
13 the Consent & Information Sharing Work Group, and has been approved by the Group. The  
14 Public Comment and Intellectual Property Rights Review has been completed. It has been  
15 approved by the Membership of the Kantara Initiative. See the Kantara Initiative [Operating](#)  
16 [Procedures](#) for more information.

17 **Abstract:**

18 A Consent Receipt is record of authority granted by a Personally Identifiable Information  
19 (PII) Principal to a PII Controller for processing of the Principal's PII. The record of consent  
20 is human-readable and can be represented as standard JSON. This specification defines the  
21 requirements for the creation of a consent record and the provision of a human-readable  
22 receipt. The standard includes requirements for links to existing privacy notices & policies as  
23 well as a description of what information has been or will be collected, the purposes for that  
24 collection as well as relevant information about how that information will be used or  
25 disclosed. This specification is based on current privacy and data protection principles as set  
26 out in various data protection laws, regulations and international standards.

27 **IPR Option:**

28 Patent & Copyright: Reciprocal Royalty Free with Opt-Out to Reasonable And  
29 Non-discriminatory (RAND)

30 **Suggested Citation:**

31 *Consent Receipt Specification 1.1.0*. Kantara Initiative Consent & Information Sharing Work  
32 Group. 2018-02-20. Kantara Initiative Technical Specification Recommendation.  
33 <https://kantarainitiative.org/file-downloads/consent-receipt-specification-v1-1-0/>

# Consent Receipt Specification

---

34

## NOTICE

35 This document has been prepared by Participants of Kantara Initiative, Inc. Permission is  
36 hereby granted to use the document solely for the purpose of implementing the  
37 Specification. Entities seeking permission to reproduce portions of this document for other  
38 uses must contact Kantara Initiative to determine whether an appropriate license for such  
39 use is available.

40 Implementation or use of certain elements of this document may require licenses under third  
41 party intellectual property rights, including without limitation, patent rights. The Participants  
42 of and any other contributors to the Specification are not and shall not be held responsible in  
43 any manner for identifying or failing to identify any or all such third party intellectual property  
44 rights. This Specification is provided "AS IS," and no Participant in Kantara Initiative makes  
45 any warranty of any kind, expressed or implied, including any implied warranties of  
46 merchantability, non-infringement of third party intellectual property rights, and fitness for a  
47 particular purpose. Implementers of this Specification are advised to review Kantara  
48 Initiative's website (<http://www.kantarainitiative.org/>) for information concerning any  
49 Necessary Claims Disclosure Notices that have been received by the Kantara Initiative  
50 Board of Directors.

51 Copyright: The content of this document is copyright of Kantara Initiative, Inc.  
52 © 2017, 2018 Kantara Initiative, Inc.

53

54

# Consent Receipt Specification

---

55	<b>Contents</b>	
56	1 Introduction.....	4
57	2 Notations and Abbreviations .....	5
58	3 Terms and definitions.....	6
59	4 Elements of a Consent Receipt .....	10
60	4.1 Introduction .....	10
61	4.2 Conformance.....	10
62	4.3 Consent Receipt Transaction Fields .....	10
63	4.4 Consent Transaction Parties Fields .....	11
64	4.5 Data, Collection, and Use Fields .....	12
65	4.6 Consent Receipt data structure .....	14
66	4.7 Presentation and Delivery.....	14
67	4.8 JSON Schema .....	16
68	5 Considerations .....	19
69	5.1 General .....	19
70	5.2 Sensitive PII .....	19
71	5.3 Security and Integrity .....	19
72	6 Acknowledgements .....	21
73	7 References .....	22
74	Appendix A: Example Consent Receipts .....	24
75	Revision history.....	29
76		

# Consent Receipt Specification

---

## 77 1 INTRODUCTION

---

78 Current regulations and best practices for privacy protection include requirements for notice  
79 and consent. There is no standard or specification for an interoperable consent record. As a  
80 result, neither individuals nor organizations can easily track their consents or know who to  
81 hold accountable in the event of a violation of their consent.

82 Individuals are regularly asked for consent by organizations who want to collect information  
83 about them, usually in conjunction with the use of a service or application. Consent is  
84 provided by an individual when they agree to allow an organization to collect, use, or  
85 disclose their data, and data about them, according to a set of terms and conditions defined  
86 by the collecting organization.

87 A record of a consent enhances the ability to maintain and manage permissions for personal  
88 data by both the individual and the organization. Much like a retailer giving a customer a  
89 cash register receipt as a record of a purchase transaction, an organization should similarly  
90 create a record of a consent interaction and give it to the individual, defined here as a  
91 Consent Receipt (CR), to memorialize this interaction in a way that is useful to people. The  
92 creation and implementation of this standardized format will promote consistent consent  
93 practices, support consent management interoperability between systems, and enable proof  
94 of consent.

95 The CR elements described in this specification represent privacy-related requirements  
96 common to many jurisdictions. A JavaScript Object Notation (JSON) schema for a CR is  
97 included to enable interoperable data exchange and processing. The specification includes  
98 extension points so that implementors can incorporate information required for their  
99 particular regulatory and policy requirements.

100 The OECD Guidelines [OECD], Council of Europe Convention, and European Union Data  
101 Protection Directive [EU-DATA] relied on Fair Information Practices (FIP) as core principles.  
102 Due to the international and cross-domain use of a Consent Receipt, this document refers to  
103 the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal  
104 Data [OECD] focusing on consent using the ISO 29100 [ISO 29100:2011] lexicon.

# Consent Receipt Specification

---

## 105 2 NOTATIONS AND ABBREVIATIONS

---

106 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD",  
107 "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL"  
108 in this document are to be interpreted as described in [\[RFC 2119\]](#).

109 All JSON [\[RFC 7159\]](#) properties and values are case sensitive. JSON data structures  
110 defined by this specification MAY contain extension properties that are not defined in this  
111 specification. Any entity receiving or retrieving a JSON data structure SHOULD ignore  
112 extension properties it is unable to understand. Extension names that are unprotected from  
113 collisions are outside the scope of this specification.

114

115 The following abbreviations are used:

116 CR Consent Receipt

117 FIP Fair Information Practices

118 GDPR General Data Protection Regulation

119 JSON JavaScript Object Notation

120 JWT JSON Web Token

121 PI Personal Information

122 PII Personally Identifiable Information

# Consent Receipt Specification

---

## 123 3 TERMS AND DEFINITIONS

---

124 This specification uses terminology and definitions from *ISO/IEC 29100:2011 "Information*  
125 *Technology -- Security techniques -- Privacy Framework"* [ISO 29100:2011] and other  
126 published, FIP-based best practices, to maintain consistency with the terms commonly used  
127 in regulations. If a jurisdiction's terms are not compatible with this specification, these  
128 internationally-defined terms can be mapped to localized terms. For example, PII Principal in  
129 this document maps to the term Data Subject in European legislation. For ease of mapping  
130 and use, this document will define those terms for clarity and specificity for this specification.

131 Although this specification uses the ISO 29100 lexicon, its use of this language is not  
132 normative, and the terms should be replaced according to the jurisdiction that regulates its  
133 provision. The JSON field names are normative. The specification is based on privacy and  
134 data protection principles as set out in various data protection laws, regulations and  
135 international standards.

### 136 **Collection**

137 Receiving, creating, or obtaining data from or about a PII Principal.

### 138 **Disclosure**

139 The transfer, copy, or communication, by a PII Controller or a PII Processor acting  
140 on behalf of the PII Controller, of PII and accountability for that PII when transferred  
141 to another entity, which will become the PII Controller of that PII.

142 NOTE: When a PII Controller transfers or copies information to another entity it  
143 retains accountability for that PII. An example would be an entity using a cloud  
144 storage service for backups. We note this here because, for a PII Principal, both this  
145 'use' and actual 'disclosure' may be termed 'sharing' information. However, there are  
146 significant differences from a transparency and regulatory point of view.

### 147 **Consent**

148 A Personally identifiable information (PII) Principal's freely given, specific and  
149 informed agreement to the processing of their PII.

150 [SOURCE: ISO 29100]

### 151 **Consent Receipt**

152 A record of a consent interaction (or consent record summary linked to the record of  
153 consent) provided by a PII Principal to a PII Controller to collect, use and disclose  
154 the PII Principal's PII in accordance with an agreed set of terms.

### 155 **Consent Timestamp**

156 The time and date when consent was obtained from the PII Principal.

### 157 **Consent Type**

158 The type of the consent used by the PII Controller as their authority to collect, use or  
159 disclose PII.

# Consent Receipt Specification

---

## 160 **Explicit (Expressed) Consent**

161 The PII Principal has an opportunity to provide a specific indication that they consent  
162 to the collection of their PII for purposes that have been specified in a prior notice or  
163 are provided at the time of collection.

164 [SOURCE: Europe 5.4.4]

## 165 **Human-readable**

166 (Of text, data, etc.) in a form that can be naturally or easily read by a person  
167 (frequently in contrast to computer-readable, machine-readable).

168 [SOURCE: OXFORD]

## 169 **Implicit (Implied) Consent**

170 The PII Controller has a reasonable expectation to believe that consent already  
171 exists for the collection of the PII.

## 172 **Opt-in**

173 A process or type of policy whereby the personally identifiable information (PII)  
174 principal is required to take an action to express explicit, prior consent for their PII to  
175 be processed for a particular purpose.

176 [SOURCE: ISO 29100]

177 Note: If the PII Principal does nothing, consent will not have been obtained.

## 178 **Opt-out**

179 A process or type of policy whereby the PII principal is required to take a separate  
180 action in order to withhold or withdraw consent, or oppose a specific type of  
181 processing.

182 [SOURCE: ISO 29100]

183 Note: If the PII Principal does nothing, consent will have been deemed to have been  
184 obtained.

## 185 **Privacy Statement**

186 A notice published or provided by the PII Controller to inform the PII Principal of what  
187 will be done with their information.

188 Note: The contents of this notice may be required by regulation and may include  
189 information that is beyond the scope of this specification.

## 190 **Personally Identifiable Information (PII)**

191 Any information that (a) can be used to identify the PII Principal to whom such  
192 information relates, or (b) is or might be directly or indirectly linked to a PII Principal.

# Consent Receipt Specification

---

193 NOTE: To determine whether or not an individual should be considered identifiable,  
194 several factors need to be taken into account.

195 [SOURCE: ISO 29100]

## 196 PII Controller

197 A privacy stakeholder (or privacy stakeholders) that determines the purposes and  
198 means for processing personally identifiable information (PII) other than natural  
199 persons who use data for personal purposes.

200 NOTE: A PII controller sometimes instructs others (e.g., PII processors) to process  
201 PII on its behalf while the responsibility for the processing remains with the PII  
202 controller.

203 [SOURCE: ISO 29100]

204 Note: may also be called data controller.

## 205 PII Principal

206 The natural person to whom the personally identifiable information (PII) relates.

207 NOTE: Depending on the jurisdiction and the particular data protection and privacy  
208 legislation, the synonym “data subject” can also be used instead of the term “PII  
209 principal.”

210 [SOURCE: ISO 29100]

## 211 PII Processor

212 A privacy stakeholder that processes personally identifiable information (PII) on  
213 behalf of and in accordance with the instructions of a PII controller.

214 [SOURCE: ISO 29100]

## 215 Processing of PII

216 An operation or set of operations performed upon personally identifiable information  
217 (PII).

218 NOTE: Examples of processing operations of PII include, but are not limited to, the  
219 collection, storage, alteration, retrieval, consultation, disclosure, anonymization,  
220 pseudonymization, dissemination or otherwise making available, deletion or  
221 destruction of PII.

222 [SOURCE: ISO 29100]

## 223 Privacy Stakeholder

224 A natural or legal person, public authority, agency or any other body that can affect,  
225 be affected by, or perceive themselves to be affected by a decision or activity related  
226 to personally identifiable information (PII) processing.

227 [SOURCE: ISO 29100]

## 228 Purpose

229 1. The business, operational or regulatory requirement for the collection, use  
230 and/or disclosure of a PII Principal's data.

231 2. The reason personal information is collected by the entity.



## Consent Receipt Specification

---

232 [SOURCE: GAPP]

### 233 **Third Party**

234 A privacy stakeholder other than the personally identifiable information (PII) principal,  
235 the PII controller and the PII processor, and the natural persons who are authorized  
236 to process the data under the direct authority of the PII controller or the PII  
237 processor.

238 [SOURCE: ISO 29100]

### 239 **Sensitive PII**

240 Sensitive Categories of personal information as defined in regulation (or potentially  
241 by the PII Principal), either whose nature is sensitive, such as those that relate to the  
242 PII principal's most intimate sphere, or that might have a significant impact on the PII  
243 principal. These categories are specified as sensitive in FIP's based legislation and  
244 refer specifically to racial origin, political opinions or religious or other beliefs,  
245 personal data on health, sex life or criminal convictions and require opt-in informed  
246 consent.

247 NOTE: In some jurisdictions or in specific contexts, sensitive PII is defined in  
248 reference to the nature of the PII and can consist of PII revealing the racial origin,  
249 political opinions or religious or other beliefs, personal data on health, sex life or  
250 criminal convictions, as well as other PII that might be defined as sensitive.

251 [SOURCE: ISO 29100]

252 Sensitive Personal Information (SPI) is defined as information that if lost,  
253 compromised, or disclosed could result in substantial harm, embarrassment,  
254 inconvenience, or unfairness to an individual.

255 [SOURCE: DHS HSSPII]

256 NOTE: For this specification, 'Sensitive data' may be considered synonymous with  
257 Sensitive PII. Sensitive Data is defined in Section 2 of the Data Protection Act of the  
258 UK (<http://www.legislation.gov.uk/ukpga/1998/29/section/2>) as personal data  
259 consisting of information relating to the data subject concerning racial or ethnic  
260 origin; political opinions; religious beliefs or other beliefs of a similar nature; trade  
261 union membership; physical or mental health or other data or as defined by  
262 implementers of the specification. In the [GDPR], this is referred to as special  
263 categories of data.

### 264 **Use**

265 Any processing of PII done by a PII Controller or by a PII processor on behalf of a PII  
266 Controller.

267 NOTE: "collection, use, and disclosure" is a useful articulation of the steps in PII  
268 processing.

# Consent Receipt Specification

---

## 269 4 ELEMENTS OF A CONSENT RECEIPT

---

### 270 4.1 Introduction

271 The following sub-sections define the fields for a Consent Receipt including the  
272 corresponding JSON field names and types. This specification uses “named object” data  
273 types to describe the principal concepts within the Consent Receipt and allows for extension  
274 by implementers. See the JSON schema for object implementation.

### 275 4.2 Conformance

276 A Consent Receipt MUST include the fields defined as REQUIRED below. When using  
277 JSON, the Consent Receipt MUST also be valid per the Consent Receipt schema in Section  
278 4.8. Additional fields MAY be added as long as they don't conflict with the conformance  
279 requirements.

### 280 4.3 Consent Receipt Transaction Fields

281 This section defines the administrative fields for the consent transaction and the metadata  
282 for the overall Consent Receipt.

#### 283 4.3.1 Version

284 REQUIRED: The version of this specification to which a receipt conforms. The value  
285 MUST be “KI-CR-v1.1.0” for this version of the specification.

286 JSON: `version`, `type: string`

#### 287 4.3.2 Jurisdiction

288 REQUIRED: The jurisdiction(s) applicable to this transaction. This field MUST  
289 contain a non-empty string describing the jurisdiction(s).

290 JSON: `jurisdiction`, `type: string`

#### 291 4.3.3 Consent Timestamp

292 REQUIRED: Date and time of the consent transaction. The JSON value MUST be  
293 expressed as the number of seconds since 1970-01-01 00:00:00 GMT. ISO 8601  
294 Date and Time Format [ISO 8601] MUST be used for formatting.

295 JSON: `consentTimestamp`, `type: integer`

#### 296 4.3.4 Collection Method

297 REQUIRED: A description of the method by which consent was obtained. Collection  
298 Method is a key field for context and determining what fields MUST be used for the  
299 Consent Receipt. This field MUST contain a non-empty string.

300 JSON: `collectionMethod`, `type: string`

#### 301 4.3.5 Consent Receipt ID

302 REQUIRED: A unique number for each Consent Receipt. SHOULD use UUID-4  
303 [RFC 4122]. This field MUST contain a non-empty string.

304 JSON: `consentReceiptID`, `type: string`

## Consent Receipt Specification

---

### 305 4.3.6 Public Key

306 OPTIONAL: The PII Controller's public key.

307 JSON: `publicKey`, `type: string`

### 308 4.3.7 Language

309 OPTIONAL: Language in which the consent was obtained. MUST use ISO 639-  
310 1:2002 [ISO 639] if this field is used.

311 JSON: `language`, `type: string`

## 312 4.4 Consent Transaction Parties Fields

313 This section defines information about the parties involved in the consent process.

### 314 4.4.1 PII Principal ID

315 REQUIRED: PII Principal-provided identifier. E.g., email address, claim,  
316 defined/namespace. Consent is not possible without an identifier. This field MUST  
317 contain a non-empty string.

318 JSON: `piiPrincipalId`, `type: string`

### 319 4.4.2 piiControllers

320 REQUIRED: An array that contains one or more items where each item represents  
321 one PII Controller. It is only required for the JSON encoding of a Consent Receipt.

322 JSON: `piiControllers`, `type: array`

### 323 4.4.3 PII Controller

324 REQUIRED: Name of the first PII Controller who collects the data. This entity is  
325 accountable for compliance with the management of PII. The PII Controller  
326 determines the purpose(s) and type(s) of PII processing. There may be more than  
327 one PII Controller for the same set(s) of operations performed on the PII, in which  
328 case the different PII Controllers SHOULD be listed. For Sensitive PII, the PII  
329 Controller MUST be specified with legally required explicit notice to the PII Principal.  
330 This field MUST contain a non-empty string.

331 JSON: `piiController`, `type: string`

### 332 4.4.4 On Behalf

333 OPTIONAL: A PII Processor acting on behalf of a PII Controller or PII Processor. For  
334 example, a third-party analytics service would be a PII Processor on behalf of the PII  
335 Controller, or a site operator acting on behalf of the PII Controller.

336 JSON: `onBehalf`, `type: boolean`

### 337 4.4.5 PII Controller Contact

338 REQUIRED: Contact name of the PII Controller. This field MUST contain a non-  
339 empty string.

340 JSON: `contact`, `type: string`

## Consent Receipt Specification

---

### 341 4.4.6 PII Controller Address

342 REQUIRED: The physical address of PII controller. Postal address for contacting the  
343 PII Controller. The JSON value MUST follow the schema at  
344 <https://schema.org/PostalAddress>.

345 JSON: `address`, `type: object`

### 346 4.4.7 PII Controller Email

347 REQUIRED: Contact email address of the PII Controller. The direct email to contact  
348 the PII Controller regarding the consent or privacy contract. This field MUST contain  
349 a non-empty string.

350 JSON: `email`, `type: string`

### 351 4.4.8 PII Controller Phone

352 REQUIRED: Contact phone number of the PII Controller. The business phone  
353 number to contact the PII Controller regarding the consent. This field MUST follow  
354 RFC 3966 [RFC 5341].

355 JSON: `phone`, `type: string`

### 356 4.4.9 PII Controller URL

357 OPTIONAL: A URL for contacting the PII Controller.

358 JSON: `piiControllerURL`, `type: string`

### 359 4.4.10 Privacy Policy

360 REQUIRED: A link to the PII Controller's privacy statement/policy and applicable  
361 terms of use in effect when the consent was obtained, and the receipt was issued. If  
362 a privacy policy changes, the link SHOULD continue to point to the old policy until  
363 there is evidence of an updated consent from the PII Principal. This field MUST  
364 contain a non-empty string.

365 JSON: `policyURL`, `type: string`

## 366 4.5 Data, Collection, and Use Fields

367 This section defines the fields for services, personal information categories, attributes, PII,  
368 and PII Sensitivity.

### 369 4.5.1 services

370 REQUIRED: An array that contains one or more items where each item represents  
371 one Service. It is only required for the JSON encoding of a Consent Receipt.

372 JSON: `services`, `type: array`

### 373 4.5.2 Service

374 REQUIRED: The service or group of services being provided for which PII is  
375 collected. The name of the service for which consent for the collection, use, and  
376 disclosure of PII is being provided. This field MUST contain a non-empty string.

377 JSON: `service`, `type: string`

# Consent Receipt Specification

---

## 378 4.5.3 purposes

379 REQUIRED: An array that contains one or more items where each item represents  
380 one Purpose. It is only required for the JSON encoding of a Consent Receipt.

381 JSON: `purposes`, `type`: `array`

## 382 4.5.4 Purpose

383 OPTIONAL: A short, clear explanation of why the PII is required.

384 JSON: `purpose`, `type`: `string`

## 385 4.5.5 Purpose Category

386 REQUIRED: The reason the PII Controller is collecting the PII. Example Purpose  
387 Categories currently in use are available on the Kantara Consent & Information  
388 Sharing Work Group (CISWG) Wiki page  
389 (<https://kantarainitiative.org/confluence/x/74K-BQ>). This field MUST contain a non-  
390 empty string.

391 JSON: `purposeCategory`, `type`: `string`

## 392 4.5.6 Consent Type

393 REQUIRED: The type of the consent used by the PII Controller as their authority to  
394 collect, use or disclose PII. The field MUST contain a non-empty string and the  
395 default value is "EXPLICIT". If consent was not explicit, a description of the consent  
396 method MUST be provided. This field MUST contain a non-empty string.

397 JSON: `consentType`, `type`: `string`

## 398 4.5.7 PII Categories

399 REQUIRED: A list of defined PII categories. PII Category should reflect the category  
400 that will be shared as understood by the PII Principal. More information can be found  
401 on the Kantara Consent & Information Sharing Work Group (CISWG) Wiki page.  
402 (<https://kantarainitiative.org/confluence/x/74K-BQ>). This field MUST contain a non-  
403 empty string.

404 JSON: `piiCategory`, `type`: `array`

## 405 4.5.8 Primary Purpose

406 OPTIONAL: Indicates if a purpose is part of the core service of the PII Controller.  
407 Possible values are TRUE or FALSE.

408 JSON: `primaryPurpose`, `type`: `boolean`

## 409 4.5.9 Termination

410 REQUIRED: Conditions for the termination of consent. Link to policy defining how  
411 consent or purpose is terminated. This field MUST contain a non-empty string.

412 JSON: `termination`, `type`: `string`

## 413 4.5.10 Third Party Disclosure

414 REQUIRED: Indicates if the PII Controller is disclosing PII to a third party. Possible  
415 values are TRUE or FALSE.

# Consent Receipt Specification

416 JSON: `thirdPartyDisclosure`, type: `boolean`

## 417 4.5.11 Third Party Name

418 REQUIRED: The name or names of the third party to which the PII Processor may  
419 disclose the PII. MUST be supplied if Third Party Disclosure is TRUE and MUST  
420 contain a non-empty string.

421 JSON: `thirdPartyName`, type: `string`

## 422 4.5.12 Sensitive PII

423 REQUIRED: Indicates whether the consent interaction contains PII that is designated  
424 sensitive or not sensitive. Possible values are TRUE or FALSE. A value of TRUE  
425 indicates that data covered by the Consent Receipt is sensitive, or could be  
426 interpreted as sensitive, which indicates that there is policy information out-of-band  
427 of the Consent Receipt.

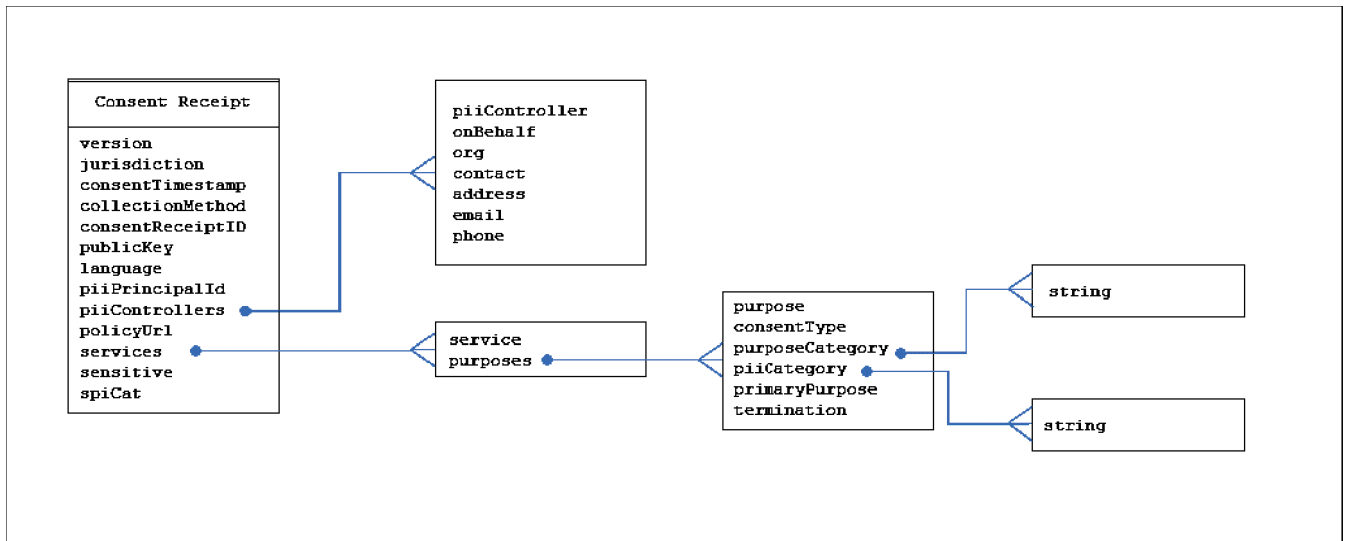
428 JSON: `sensitive`, type: `boolean`

## 429 4.5.13 Sensitive PII Category

430 REQUIRED: A listing of categories where PII data collected is sensitive. The field  
431 MUST contain a non-empty string if Sensitive PII is TRUE.

432 JSON: `spiCat`, type: `array`

## 433 4.6 Consent Receipt data structure



434

435 Figure 1

## 436 4.7 Presentation and Delivery

437 Although a CR can be provisioned in any manner that is feasible or expected based on the  
438 context, a CR MUST be provided to the PII Principal in a human-readable format either on  
439 screen or delivered to the PII Principal, or both. A JSON encoded CR MAY also be delivered  
440 to the PII Principal.

## Consent Receipt Specification

---

441 We note that in some use cases, the PII Controller may primarily depend upon a proprietary  
442 consent management system that may display a receipt on demand. So long as the  
443 presentation UI contains the information set out in this standard, it will be deemed to be a  
444 human-readable Consent Receipt.

445 NOTE: Issues such as language translation, localization, human-readable layout and  
446 formatting, and delivery mechanisms are out-of-scope for this document.

447

# Consent Receipt Specification

## 448 4.8 JSON Schema

```
449 {
450   // Kantara Consent Receipt Specification v 1.1.0 DRAFT 6
451   //2017-11-17
452
453   "$schema": "http://json-schema.org/draft-04/schema#",
454   "type": "object",
455   "properties": {
456     "version": {
457       "type": "string"
458     },
459     "jurisdiction": {
460       "type": "string"
461     },
462     "consentTimestamp": {
463       "type": "integer",
464       "minimum": 0
465     },
466     "collectionMethod": {
467       "type": "string"
468     },
469     "consentReceiptID": {
470       "type": "string"
471     },
472     "publicKey": {
473       "type": "string"
474     },
475     "language": {
476       "type": "string"
477     },
478     "piiPrincipalId": {
479       "type": "string"
480     },
481     "piiControllers": {
482       "type": "array",
483       "items": {
484         "type": "object",
485         "properties": {
486           "piiController": {
487             "type": "string"
488           },
489           "onBehalf": {
490             "type": "boolean"
491           },
492           "contact": {
493             "type": "string"
494           },
495           "address": {
496             "type": "object"
497           },
498           "email": {
499             "type": "string"
500           },
501           "phone": {
502             "type": "string"
503           },
504           "piiControllerUrl": {
505             "type": "string"
506           }
507         },
508         "required": [
509           "piiController",
```



# Consent Receipt Specification

```
510         "contact",
511         "address",
512         "email",
513         "phone"
514     ]
515     },
516     },
517     "policyUrl": {
518         "type": "string"
519     },
520     "services": {
521         "type": "array",
522         "items": {
523             "type": "object",
524             "properties": {
525                 "service": {
526                     "type": "string"
527                 },
528                 "purposes": {
529                     "type": "array",
530                     "items": {
531                         "type": "object",
532                         "properties": {
533                             "purpose": {
534                                 "type": "string"
535                             },
536                             "consentType": {
537                                 "type": "string"
538                             },
539                             "purposeCategory": {
540                                 "type": "array",
541                                 "items": {
542                                     "type": "string"
543                                 }
544                             },
545                             "piiCategory": {
546                                 "type": "array",
547                                 "items": {
548                                     "type": "string"
549                                 }
550                             },
551                             "primaryPurpose": {
552                                 "type": "boolean"
553                             },
554                             "termination": {
555                                 "type": "string"
556                             }
557                         }
558                     },
559                     "oneOf": [
560                         {
561                             "properties": {
562                                 "thirdPartyDisclosure": {
563                                     "type": "boolean",
564                                     "enum": [
565                                         false
566                                     ]
567                                 }
568                             },
569                             "required": [
570                                 "thirdPartyDisclosure"
571                             ]
572                         }
573                     ],
574                     "properties": {
```

## Consent Receipt Specification

```
574         "thirdPartyDisclosure": {
575             "type": "boolean",
576             "enum": [
577                 true
578             ]
579         },
580         "thirdPartyName": {
581             "type": "string"
582         }
583     },
584     "required": [
585         "thirdPartyDisclosure",
586         "thirdPartyName"
587     ]
588 },
589 ],
590 "required": [
591     "consentType",
592     "purposeCategory",
593     "piiCategory",
594     "termination",
595     "thirdPartyDisclosure"
596 ]
597 }
598 },
599 },
600 "required": [
601     "service",
602     "purposes"
603 ]
604 }
605 },
606 "sensitive": {
607     "type": "boolean"
608 },
609 "spiCat": {
610     "type": "array",
611     "items": {
612         "type": "string"
613     }
614 }
615 },
616 "required": [
617     "version",
618     "jurisdiction",
619     "consentTimestamp",
620     "collectionMethod",
621     "consentReceiptID",
622     "piiPrincipalId",
623     "piiControllers",
624     "services",
625     "policyUrl",
626     "sensitive",
627     "spiCat"
628 ]
629 }
```

# Consent Receipt Specification

---

## 630 5 CONSIDERATIONS

---

### 631 5.1 General

632 Consent is a means for people to regulate their privacy in a specific context. As a social  
633 control, consent is a signal people provide when they share personal information specific to  
634 that context. Since the scope of each context will vary, different Consent Receipt  
635 implementations will have different requirements for user experience, legal, privacy, and  
636 security-related considerations for the collection disclosure and use of PII consent by the PII  
637 Controller.

### 638 5.2 Sensitive PII

639 In some jurisdictions there are categories listed as sensitive personal information. If the use,  
640 collection or disclosure of sensitive personal information has legal requirements as defined  
641 in regulation, explicit consent is probably required with jurisdiction-specific legal notice  
642 requirements. For example, PII revealing the racial origin, political opinions or religious or  
643 other beliefs, personal data on health, sex life or criminal convictions, as well as other PII  
644 that are defined as sensitive in regulation.

### 645 5.3 Security and Integrity

#### 646 5.3.1 Overview

647 Since Consent Receipts can contain PII, it is a requirement that transmission of Consent  
648 Receipts does not take place in the clear and that secure communications be used, e.g.,  
649 HTTPS. The requirements for implementers of Consent Receipts and consent management  
650 solutions include signing, encryption, key management and other operations for their  
651 creation, transmission, use, and storage if the Consent Receipt is to be used for proof of  
652 consent, withdrawal of consent or any other rights.

#### 653 5.3.2 Guidance

- 654 1. Ensure the use of securely authenticated connections using modern cryptology.
- 655 2. If a receipt contains PII - a receipt without PII is not in scope here - and it is  
656 transmitted securely, the user must be able to manage the receipt interactions with:
  - 657 a. Storage (local machine, server, client, application, device, etc.)
  - 658 b. Other receipt repositories and consent services.
    - 659 i. Security of these repositories and services - i.e., non-local, requires  
660 considerations but is currently out-of-scope of this specification.
    - 661 ii. When considered it should include the use case where for some  
662 reason a receipt has not been transmitted it should be available from  
663 the provider of the receipt repository for direct download. Such  
664 infrastructure is out-of-scope for this specification.
  - 665 c. Transmission of receipts with PII.
- 666 3. The ability to validate and revoke the receipt – and other aspects of the Consent  
667 Receipt lifecycle are out-of-scope for this specification at this time but will need to be  
668 taken up shortly. Additional topics for future consideration include:
  - 669 a. Consent best practices.
  - 670 b. Status and revocation of consent.
  - 671 c. Consent management, validation, and other aspects of its lifecycle.

## Consent Receipt Specification

---

- 672 The transmission of a JSON Consent Receipt should use the following specifications:
- 673       JSON Web Token (JWT) [RFC 7519]
- 674       JSON Web Encryption (JWE) [RFC 7516]
- 675       JSON Web Signature (JWS) [RFC 7515]

# Consent Receipt Specification

---

## 676 6 ACKNOWLEDGEMENTS

---

677 The Consent Receipt effort has been developed in the Kantara Community, supported by  
678 people who have invested in making this specification open and free to use. It is free so that  
679 people can have a common way to see what consents have been provided and what data is  
680 being shared or disclosed. If you wish to provide feedback, you may join the Kantara  
681 Working Group, and then email us on our list at [wg-infosharing@kantarainitiative.org](mailto:wg-infosharing@kantarainitiative.org) or  
682 send feedback to [staff@kantarainitiative.org](mailto:staff@kantarainitiative.org) .

683 In addition to Kantara, we wish to thank the following contributors to the Consent Receipt  
684 effort:

685 Customer Commons

686 Colin Wallis

687 Justin Richer

688 Sarah Squire

689 Eve Maler

690 Joss Langford

691 Thomas Lenggenhager

692 Tom Jones

693 Barry Hieb

694 The Consent Receipt standardization effort has been developed with the support of many  
695 communities, as noted in our acknowledgments section, and leverages best of breed  
696 standards, legal regulation and technical practices in its design and development, as noted  
697 in the references section.

# Consent Receipt Specification

698

## 7 REFERENCES

- 699 **[DHS HSSPII]** *DHS Handbook for Safeguarding Sensitive PII*. (Ed. 2012).  
700 [https://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguarding-sensitive-PII\\_march\\_2012\\_webversion.pdf](https://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguarding-sensitive-PII_march_2012_webversion.pdf)  
701
- 702 **[EU-DATA]** Directive 95/46/EC of the European Parliament and of the Council of 24 October  
703 1995 on the protection of individuals with regard to the processing of personal data and on  
704 the free movement of such data. [http://eur-lex.europa.eu/legal-](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046)  
705 [content/EN/TXT/?uri=CELEX:31995L0046](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046)
- 706 **[Europe 5.4.4]** Kosta, E., *Consent in European Data Protection Law*. Section 5.4: “Consent  
707 in the Context of Sensitive Data.” (Ed: 2013) p. 98-100. <https://goo.gl/JGPX2Y>
- 708 **[GAPP]** *Generally Accepted Privacy Principles* - developed through joint consultation with  
709 the Canadian Institute of Chartered Accountants (CICA) and the American Institute of  
710 Certified Public Accountants (AICPA) through the AICPA/CICA Privacy Task Force.  
711 <https://www.cippguide.org/2010/07/01/generally-accepted-privacy-principles-gapp/>
- 712 **[GDPR]** *General Data Protection Regulation*, <http://www.eugdpr.org/article-summaries.html>
- 713 **[ISO 639]** ISO 639-1:2002, *Codes for the representation of names of languages — Part 1:*  
714 *Alpha-2 code* <https://www.iso.org/standard/22109.html>
- 715 **[ISO 18001-1:2005]** *Information technology — Personal identification — ISO-compliant*  
716 *driving license — Part 1: Physical characteristics and basic data set.*  
717 <https://www.iso.org/obp/ui/#iso:std:iso-iec:18013:-1:ed-1:v1:en>
- 718 **[ISO 29100:2011]** *Information technology -- Security techniques -- Privacy framework.*  
719 [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=45123](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123)
- 720 **[PIPEDA]** *Personal Information Protection and Electronic Documents Act*, [http://laws-](http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html)  
721 [lois.justice.gc.ca/eng/acts/P-8.6/index.html](http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html)
- 722 **[RFC 2119]** Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, BCP  
723 14, RFC 2119, DOI 10.17487/RFC2119, March 1997 <http://www.rfc-editor.org/info/rfc2119>
- 724 **[RFC 5341]** C. Jennings, V. Gurbani, “The Internet Assigned Number Authority (IANA) tel  
725 Uniform Resource Identifier (URI) Parameter Registry”, RFC 5341, DOI:  
726 10.17487/RFC5341, September 2008, <https://tools.ietf.org/html/rfc5341>
- 727 **[RFC 4122]** P. Leach, M. Mealling, R. Salz, “A Universally Unique Identifier (UUID) URN  
728 Namespace”, RFC 4122, 10.17487/RFC4122, July 2005, <https://tools.ietf.org/html/rfc4122>
- 729 **[RFC 7159]** Bray, T., Ed., “The JavaScript Object Notation (JSON) Data Interchange  
730 Format”, RFC 7159, DOI 10.17487/RFC7159, March 2014, [http://www.rfc-](http://www.rfc-editor.org/info/rfc7159)  
731 [editor.org/info/rfc7159](http://www.rfc-editor.org/info/rfc7159)
- 732 **[RFC 7515]** M. Jones, J. Bradley, N. Sakimura, “JSON Web Signature (JWS)”, RFC 7515,  
733 May 2015, <https://tools.ietf.org/html/rfc7515>
- 734 **[RFC 7516]** M. Jones, J. Hildebrand, “JSON Web Encryption (JWE)”, RFC 7516, May 2015,  
735 <https://tools.ietf.org/html/rfc7516>
- 736 **[RFC 7519]** M. Jones, J. Bradley, N. Sakimura, “JSON Web Token (JWT)”, RFC 7519, DOI  
737 10.17487/RFC7519, May 2015, <https://tools.ietf.org/html/rfc7519>

## Consent Receipt Specification

---

- 738 **[OECD]** *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal*  
739 *Data.*  
740 [http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflo](http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflows)  
741 [wsofpersonaldata.htm](http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflows)
- 742 **[OXFORD]** Oxford University Press - Definition of human-readable in English,  
743 <https://en.oxforddictionaries.com/definition/us/human-readable>

# Consent Receipt Specification

744

## APPENDIX A: EXAMPLE CONSENT RECEIPTS

745

### A.1 Human-readable Consent Receipt – Simple

Consent Receipt <sup>1</sup>	
<i>Version</i>	KI-CR-v1.1.0
<i>Jurisdiction</i>	Discworld
<i>Consent Timestamp</i>	11/13/2017, 12:00:00 PM EST
<i>Collection Method</i>	Web Subscription Form with opt-in for marketing
<i>Consent Receipt ID</i>	c1befd3e-b7e5-4ea6-8688-e9a565aade21
<i>Public Key</i>	04:a3:1d:40:53:f0:4b:f1:f9:1b:b2:3a:83:a9:d1: 40:02:cc:31:b6:4a:77:bf:5e:a0:db:4f:ea:d2:07: c4:23:57:6f:83:2c:3d:3e:8d:e7:02:71:60:54:01: f4:6a:fb:a2:1e:8b:42:53:33:78:68:d9:7d:5e:b2: cc:0b:f8:a1:bf
<i>Language</i>	English
<b>Consent Parties</b>	
<b>Information Subject</b>	
<i>PII Principle ID</i>	<b>Bowden Jeffries</b>
<b>Information Controller</b>	
<i>PII Controller Name</i>	<b>Ankh-Morpork Times</b>
<i>PII Controller Contact</i>	William de Word, Chief Editor & Data Protection Officer
<i>PII Controller Address</i>	Ankh-Morpork Times Gleam Street, Ankh-Morpork, Discworld
<i>PII Controller Email</i>	william@times.ankh-morpork.xyz
<i>PII Controller Phone</i>	(555) 555-DISC (3429)
<i>PII Controller URL</i>	<a href="https://www.times.ankh-morpork.xyz/contact">https://www.times.ankh-morpork.xyz/contact</a>
<i>Privacy Policy</i>	<a href="https://times.ankh-morpork.zxy/privacy_2017">https://times.ankh-morpork.zxy/privacy_2017</a>

Please see the next page for details on the data we have collected about you, and what we will do with it.

<sup>1</sup> Sample Consent Receipt, version 1.1.0

746

747



# Consent Receipt Specification

Data, collection and use				
Service		Digital Subscription and News Alerts		
Purposes for collection and use				
Purpose	Purpose Category	Consent Type	PII Categories	Primary purpose?
Fulfil Digital Subscription	Provision of services	EXPLICIT	<ul style="list-style-type: none"> <li>Technical</li> <li>Demographics</li> <li>Financial</li> <li>Contact</li> </ul>	TRUE
Marketing	Marketing	EXPLICIT	<ul style="list-style-type: none"> <li>Demographics</li> <li>Financial</li> <li>Contact</li> </ul>	FALSE
Financial Record Keeping	Fiduciary obligation	N/A	<ul style="list-style-type: none"> <li>Financial</li> </ul>	FALSE
Law Enforcement	Legal obligation	N/A	<ul style="list-style-type: none"> <li>All</li> </ul>	FALSE
Termination				
	<a href="https://times.ankh-morpork.zxy/privacy_2017#termination">https://times.ankh-morpork.zxy/privacy_2017#termination</a>			
Third Party Disclosure		True		
Third Party Names		<ul style="list-style-type: none"> <li>Outsourced printer</li> <li>Outsourced fulfillment vendor</li> <li>Bank</li> <li>Law enforcement with subpoena</li> <li>Digital Advertising Agency</li> </ul>		
Sensitive PII		Yes		
Sensitive PII Category		Financial Information		

748  
749

# Consent Receipt Specification

750

## A.2 Human-readable Consent Receipt – Fancy

### Receipt for Personally Identifiable Information

Service: Digital Subscription and News Alerts

At the Ankh-Morpork Times we take your privacy seriously. This document is being provided to you as a receipt for personally identifiable information that we have, or will collect about you. It tells you what information has been collected and for what purposes we will use and disclose it. For your information, this document is based on the Consent Receipt Specification v1.1.0 published by the Kantara Initiative.

We have collected, or will collect, the information described below based on your implicit consent when you completed our web subscription form. If you receive marketing material, it will be because you ticked an opt-in check box for marketing. We operate and follow the data protection rules for DiscWorld (dw). We will continue to collect and use your information until 1 year after your subscription ends.

**YOUR ID: BOWDEN JEFFRIES**

#### Types of Information we have or may collect about you<sup>f</sup>.

#### The purposes for collection of your personal information<sup>o,n</sup>.

General biographical information about you (demographics)  
Your financial information for payments<sup>s</sup>  
Your contact information

Technical data for web servers (Core Function)  
News web site and alerts (Contracted Service)  
Marketing<sup>o</sup>  
Meeting Fiduciary & Legal Obligations<sup>n</sup>

About Us: The Ankh-Morpork Times is the Personally Identifiable Information Controller that is accountable for the information that has been collected about you. We are acting on our own behalf. For more details on our privacy notice and practices see the privacy policy linked to below.

<i>Our Contact Information</i>	The Ankh-Morpork Times Gleam Street, Ankh-Morpork, Discworld <a href="https://www.times.ankh-morpork.xyz/contact">https://www.times.ankh-morpork.xyz/contact</a>
<i>Privacy Contact</i>	William de Worde, Chief Editor and Privacy Officer <a href="mailto:william@times.ankh-morpork.xyz">william@times.ankh-morpork.xyz</a> (555) 555-DISC (3429) x 7748229 (Privacy)
<i>Privacy Policy</i>	<a href="https://times.ankh-morpork.zxy/privacy_2017">https://times.ankh-morpork.zxy/privacy_2017</a>

Third parties how may receive information about you:

Outsourced printer                      Bank                      Digital Advertising Agency  
Outsourced fulfillment vendor              Law enforcement with subpoena

Receipt #: c1befd3e-b7e5-4ea6-8688-e9a565aade21  
Date: 11/13/2017, 12:00:00 PM EST

<sup>s</sup> Information marked with a superscript s may be treated as "Sensitive Personal Information"

<sup>o</sup> Purposes marked with a superscript o indicated an optional consent.

<sup>n</sup> Purposes marked with a superscript n do not require consent

751

752

# Consent Receipt Specification

## 753 A.3 JSON Consent Receipt

```
754 {
755   "version": "KI-CR-v1.1.0",
756   "jurisdiction": "DW",
757   "consentTimestamp": 1510592400,
758   "collectionMethod": "Web Subscription Form with opt-in for marketing",
759   "consentReceiptID": "c1befd3e-b7e5-4ea6-8688-e9a565aade21",
760   "publicKey":
761     "04:a3:1d:40:53:f0:4b:f1:f9:1b:b2:3a:83:a9:d1:\r\n40:02:cc:31:b6:4a:77:bf:5
762     e:a0:db:4f:ea:d2:07:\r\n4c:23:57:6f:83:2c:3d:3e:8d:e7:02:71:60:54:01:\r\nf4
763     :6a:fb:a2:1e:8b:42:53:33:78:68:d9:7d:5e:b2:\r\ncc:0b:f8:a1:bf",
764   "language": "en",
765   "piiPrincipalId": "Bowden Jeffries",
766   "piiControllers": [
767     {
768       "piiController": "Ankh-Morpork Times",
769       "contact": "William De Worde",
770       "address": {
771         "streetAddress": "Gleam Street",
772         "addressCountry": "DW"
773       },
774       "email": "william@times.ankh-morpork.xyz",
775       "phone": "(555) 555-DISC (3429)"
776     }
777   ],
778   "policyUrl": "https://times.ankh-morpork.xzy/privacy_2017",
779   "services": [
780     {
781       "service": "Digital Subscription and News Alerts",
782       "purposes": [
783         {
784           "purpose": "To provide contracted services",
785           "purposeCategory": [
786             "2 - Contracted Service"
787           ],
788           "consentType": "EXPLICIT",
789           "piiCategory": [
790             "1 - Biographical",
791             "2 - Contact",
792             "4 - Communications/Social",
793             "7 - Financial"
794           ],
795           "primaryPurpose": true,
796           "termination": "Subscription end date + 1 year",
797           "thirdPartyDisclosure": true,
798           "thirdPartyName": "The Ankh-morpork Deadbeat Debt Collectors
799 Society"
800         },
801         {
802           "purpose": "To personalize service experience",
803           "purposeCategory": [
804             "5 - Personalize Experience"
805           ],
806           "consentType": "EXPLICIT",
807           "piiCategory": [
808             "1 - Biographical",
809             "2 - Contact",
810             "4 - Communications/Social"
811           ],
812           "primaryPurpose": false,
813           "termination": "Subscription end date + 1 year",
814           "thirdPartyDisclosure": false

```

## Consent Receipt Specification

---

```
815     },
816     {
817         "purpose": "To market services",
818         "purposeCategory": [
819             "6 - Marketing"
820         ],
821         "consentType": "EXPLICIT",
822         "piiCategory": [
823             "2 - Contact"
824         ],
825         "primaryPurpose": false,
826         "termination": "Subscription end date + 1 year",
827         "thirdPartyDisclosure": false,
828         "thirdPartyName": "DiscWorld Octarine Programmatic Ad Agency"
829     },
830     {
831         "purpose": "Complying with legal obligations",
832         "purposeCategory": [
833             "12 - Legally Required Data Retention",
834             "13 - Required by Law Enforcement or Government"
835         ],
836         "consentType": "N/A",
837         "piiCategory": [
838             "1 - Biographical",
839             "2 - Contact",
840             "4 - Communications/Social",
841             "7 - Financial"
842         ],
843         "primaryPurpose": false,
844         "termination": "N/A",
845         "thirdPartyDisclosure": true,
846         "thirdPartyName": "Requesting legal authority"
847     }
848 ]
849 }
850 ],
851 "sensitive": true,
852 "spiCat": [
853     "1 - Biographical",
854     "7 - Financial"
855 ]
856 }
```

# Consent Receipt Specification

857

## REVISION HISTORY

Version	Date	Summary of Substantive Changes
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	2018-02-15	Revisions based on comment from public review period.
1.1.0	2018-05-02	Candidate Kantara Initiative Technical Specification Recommendation
1.1.0	2018-05-25	Final Recommendation approved by Kantara All-Member Ballot

858

859