



Implementing ISO/IEC TS 27560:2023 Consent Records and Receipts for GDPR and DGA

Harshvardhan J. Pandit^{1,2} , Jan Lindquist³, and Georg P. Krog⁴

¹ ADAPT Centre, Dublin City University, Dublin, Ireland
me@harshp.com

² Cybersecurity and Data Protection Group, National Standards Institute,
Dublin, Ireland

³ Privacy and Security Group, Institute for Standards, Stockholm, Sweden
jan@linaltec.com

⁴ Signatu AS, Oslo, Norway
georg@signatu.com

Abstract. The ISO/IEC TS 27560:2023 Privacy technologies—Consent record information structure provides guidance for the creation and maintenance of records regarding consent as machine-readable information. It also provides guidance on the use of this information to exchange such records between entities in the form of ‘receipts’. In this article, we compare requirements regarding consent between ISO/IEC TS 27560:2023, ISO/IEC 29184:2020 Privacy Notices, and the EU’s General Data Protection Regulation (GDPR) to show how these standards can be used to support GDPR compliance. We then use the Data Privacy Vocabulary (DPV) to implement ISO/IEC TS 27560:2023 and create interoperable consent records and receipts. We also discuss how this work benefits the implementation of EU Data Governance Act (DGA), specifically for machine-readable consent forms.

Keywords: consent · consent receipt · GDPR · DGA · ISO · Semantics

1 Introduction

Informed Consent is an important legal basis as it provides control and empowerment to data subjects or users based on the ability to choose and make decisions. Privacy and data protection laws such as EU’s GDPR [16] regulate this process by defining conditions for when consent should be considered *Valid Consent*. The process of *Informed Consent* requires information be provided in the form of a *Consent Notice* to inform the data subject about the processing that will occur based on the consent and to enable them to make an *informed choice or decision*.

In order to assess whether an instance of given consent is valid thus requires keeping records of information regarding how the consent was obtained i.e. using

the notice, and how the consent is being utilised i.e. the processing enabled through that consent. This same information is also required for the organisation to determine whether its processing activities should continue, e.g. depending on whether a particular user has given consent and whether it is still valid i.e. hasn't expired or wasn't withdrawn). Such information that is documented and maintained regarding consent is called a *Consent Record*.

ISO/IEC TS 27560:2023 Consent record information structure [6] is a Technical Specification that “specifies an interoperable, open and extensible information structure” for recording the data subject’s consent to processing of their personal data i.e. as consent records, and to provide this information i.e. as consent receipts. The specification lists *information fields* that represent specific information associated with consent, and requirements over the form this information can take e.g. format, number of values, and whether it is mandatory or optional. It complements the earlier ISO/IEC 29184:2020 Online privacy notices and consent [5] which describes the information to be provided within privacy notices.

A ISO-27560 conformant implementation fulfils requirements by either storing information directly in the form prescribed by ISO-27560 or by storing information in a form that can be used to obtain this information. ISO-27560 allows flexibility in how the fields are represented to suit and match domain-specific labels or descriptions, or to introduce additional fields or information types that are needed. Such changes, expressed as *schemas* or *profiles*, are still required to be compatible with the requirements of ISO-27560 such as by requiring the same fields to be mandatory. In this manner, ISO-27560 provides a common, interoperable, and extensible structure for the exchange of information associated with consent.

In this article, we present an analysis of the requirements for recording consent within ISO-27560 and ISO-29184 and compare them with the requirements for valid consent under GDPR (Sect. 3). We then present our work in implementing ISO-27560 using the Data Privacy Vocabulary (DPV) [13, 15] to create a machine-readable, interoperable, and extensible specification for consent records and receipts based on open standards (Sect. 4). Through this work we demonstrate the applicability and usefulness of ISO-27560 in assisting with the obligation for demonstrating consent under GDPR (Art. 7-1), and explore how ISO-27560 and ISO-29184 can work within the legal framework of GDPR and DGA and the possibility for using this standard to inform the implementation of machine-readable common consent forms under the DGA (Sect. 5). We also discuss practicalities for implementations regarding trust and security (Sect. 6.1) and using records and receipts with eIDAS and EUDI wallets (Sect. 6.2).

2 Overview of ISO/IEC TS 27560:2023

Goals and Scope. ISO-27560 has two broad goals: to guide the recording of information about consent for processing of personal data in a form that is interoperable, open, and extendable, and to provide information to individuals. To

implement this, it defines several requirements (as *controls* in ISO terminology) for ensuring the required information is maintained and is supported by appropriate processes within the organisation. ISO-27560 is stated as a supplement to the earlier ISO-29184, where ISO-29184 defines how information is provided via notices in order to request consent, and ISO-27560 defines how information is recorded for given consent and provided back to the individual (as receipts).

The objective of ISO-27560 is to define an information structure for consent record which contains: (1) Information about the processing of personal data; (2) Privacy notices where this information was provided; (3) How data was obtained; and (4) Events related to consent (giving, withdrawing, etc.). It also defines an information structure providing all or some of this information to the data subject in the form of a consent receipt. To support implementations, Annex A provides examples of consent records and receipts using DPV, and Annex B provides an overview of the different states or stages in 'consent lifecycle' - which is based on DPV's consent states [13, 15] and analysis of existing approaches [2, 8].

Specific guidance on implementation such as the choice of technologies is not in the scope of ISO-27560, though its Annexes provide informative guidance on related topics. Annex C describes performance and efficiency considerations, Annex D describes format and encoding structures, Annex E describes security of records and receipts, and Annex G describes application in Privacy Information Management Systems (PIMS). Further uses of consent records or receipts, such as how data subjects can obtain consent receipts or maintain their own consent records is not described in ISO-27560.

Consent Records. ISO-27560 defines *Consent Record* as the documentation of information about a data subject's consent for the processing of their personal data in terms of the details about the processing as well as the interactions related to consent (e.g. giving or withdrawing it). Consent Records are an essential part of keeping records regarding whether consent has been obtained and is valid for processing, and to keep this information for correctly conducting processing relying on it. ISO-27560 as well as regulatory requirements such as GDPR Article 7-1 require maintaining consent records where consent is used as the legal basis. While GDPR Article 7-1 only states that consent should be demonstrable, ISO-27560 provides an information structure for how this information should be maintained and what processes should exist within an organisation in for this.

It is important to distinguish between a *Consent Record* with several relevant but distinct concepts. A consent record only refers to the information recorded regarding consent, whereas a *Consent Notice* refers to the notice and information provided to the data subject in order to inform them about the processing - such as while requesting consent. While there is a significant overlap between a consent record and a consent notice, there are key differences such as notices orienting information for human consumption (e.g. layering of dialogues to provide summaries and detailed descriptions) and dictating the manner in which consent is expressed (e.g. checkboxes for options and confirmation by clicking a button). In contrast, a consent record is not required to accurately reflect the

manner in which this information was presented to the user, but to only record it in a manner that enables assessing whether the consent is given and if so for which processing activities.

This distinction is evident in ISO-29184 being the standard for consent notices - which specifies what information should be present in a notice and the manner in which it is presented. In turn, ISO-27560 only refers to notices to limit its scope to representing information necessary within a consent record. Therefore a consent record, despite containing a link to the notice, is not by itself sufficient to determine the *validity* of consent, and instead acts as the primary record containing information or links to information for conducting such assessments. Its primary purpose is therefore limited to supporting claims for who is the subject, who is the controller, what is the consent about (e.g. which purpose, what recipients), what is the state of consent (e.g. request, given, terminated), and where/when/how it occurred (e.g. accepted on specific timestamp).

A ISO-27560 conformant consent record typically has the following sections representing relevant information:

1. metadata about the consent record such as its identifier
2. the individual associated with the consent i.e. data subject
3. the subject of consent i.e. specifics of the processing of personal data such as purposes, services, data categories, and storage conditions
4. entities involved e.g. data controller and third parties
5. relevant contextual information e.g. notice, rights, restrictions
6. provenance of events associated with the consent e.g. given, withdrawn

Under GDPR, the obligation to maintain records of consent is explicitly stated in Article 7-1 and Recital 42. This information includes, at a minimum, the identity of the Controller and the purposes of processing (Recital 42). Further, Articles 13 and 14 dictate the information that must be provided to the data subject which includes recipients, transfers to third countries, data storage periods and conditions, existence of rights (including consent withdrawal), and specific information regarding processing such as the use of automated decision making or profiling.

Consent Receipts. ISO-27560 defines a consent receipt as an authoritative document that is used to communicate the existence of a consent record or to provide information contained within it. It is effectively an 'authoritative copy' of a consent record provided by one entity to another, where it may contain all or only some information from the consent record regarding the consent and its relevance to processing activities. Such receipts are useful to communicate the existence of consent decisions, and enable entities to exercise of rights or raise issues and complaint regarding processing activities.

Consent receipts are a relatively newer and under-utilised practice, with no legal requirements existing that refer to the concept (of receipts) or state how they should be used. In addition, the usefulness of receipts as information provided to another entity requires consideration of specific terms and norms particular to the domain or sector. ISO-27560 follows this by providing the flexibility

for organisations to choose a suitable schema for their particular domain or use-case. It defines a minimal structure consisting of some fields representing the receipt metadata, but does not have any requirements on the information structuring within the receipt or its correspondence to fields within the record.

A ISO-27560 conformant consent receipt only requires a metadata section providing information about the consent receipt such as its identifier. Deciding on which additional information is to be provided and in what forms and using which structures is left up to implementing entities. In this guide, we presume that the consent receipt is intended for providing a copy of all information within the consent record.

According to ISO-27560, records are generated and maintained by organisations (Controller, Third Party), and are utilised to provide receipts to a Data Subject. In contrast, the Kantara Consent Receipts specification [9], upon which ISO-27560 is based, defines Consent Receipts as being provided by a Data Subject to a Controller.

For practical considerations of this work, we make no presumptions or enact restrictions on the use of records and receipts. Any entity, be it a Controller or a Data Subject, can maintain their own consent record or issue receipts. Though the phrasing of some sections may imply the Controller as the implementing entity, it does not preclude another entity from also implementing ISO-27560.

Structure. A Consent Record contains four sections as described below and depicted visually in Fig. 1 (the terms used are based on the implementation of ISO-27560 for GDPR using DPV as described later in the article):

1. **Header Fields:** these provide metadata about the record e.g. its unique identifier and timestamp of creation. These fields also include information on the schema which dictates how the information in the record is structured and which fields are necessary/optional. ISO-27560 permits creation of different schemas to support varying use-cases and information requirements.
2. **Processing Fields:** these provide information about the processing activities e.g. purposes, personal data, storage durations, geographic locations and restrictions, link to privacy notice, rights, and others.
3. **Parties Fields:** these provide information about entities involved in the processing e.g. controllers, third parties, authorities. The party has an identifier which is used to link or associate it with fields in the processing section e.g. to indicate which party is the controller.
4. **Events Fields:** these provide information about *consent events* e.g. consent given, consent withdrawn. Information includes the type of event, time, duration, associated entity, and how it was expressed.

Each section contains fields which describe the information that must be represented along with the form (e.g. timestamp format) and its necessity (e.g. required or optional). Certain fields are expressed as references to other fields (e.g. ‘Controller’ in ‘Processing’ section is a reference to an instance or record in ‘Parties’ section).

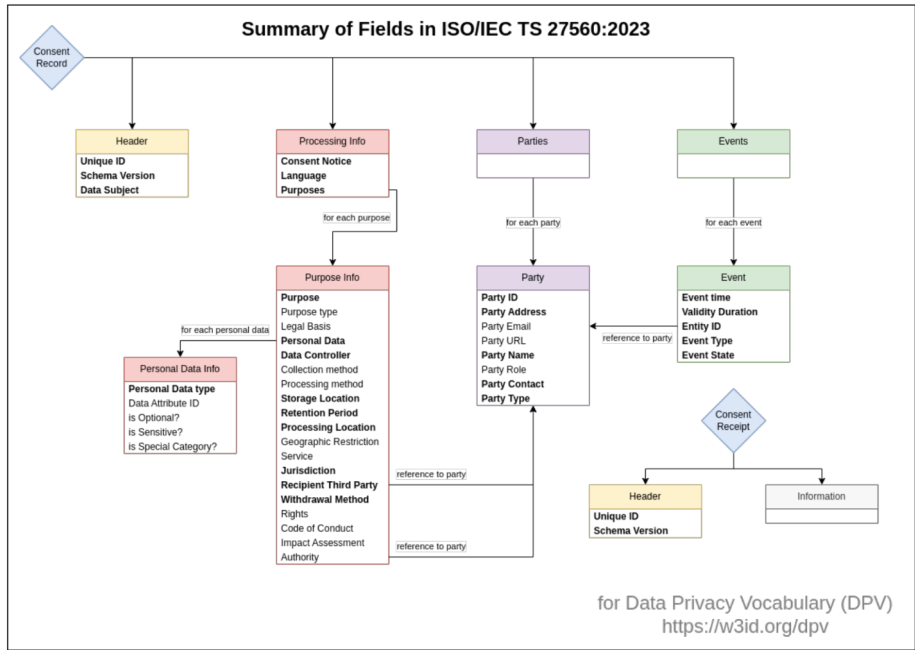


Fig. 1. Summary of fields in ISO/IEC TS 27560:2023. The field names have been modified for alignment with DPV concepts. Field names in bold are mandatory.

The Consent Receipt in ISO-27560 contains only two required fields representing a unique identifier for the receipt and the schema version used for the structuring of information. The information and contents are undefined and left to each implementor to specify. A receipt can optionally contain the entirety of the information within a consent record or can also contain multiple consent records or other information not within a particular consent record. Similarly, a receipt can be made to contain only references to information within a record without containing the information itself e.g. providing only the consent record identifier without the contents of the record itself.

Considering the practical application of consent receipts require them to provide information to data subjects, for the implementation described in this document, it is assumed that the consent receipt provides all information contained within a consent record i.e. a receipt is a copy of the record provided to another entity. This is in line with ISO-27560 guidance which states that the receipt may contain the same fields as that of a consent record, and that the mandatory fields in a consent record are also mandatory in a consent receipt. Further, ISO-27560 allows creating different ‘schemas’ (which we call ‘profiles’) to indicate changes in requirements and their interpretations, through which we provide profiles for our defined implementations.

3 Comparing ISO-27560, ISO-29184, and GDPR

ISO-27560 uses prior terminology established in ISO standards, primarily defined in ISO/IEC 29100:2011 Privacy Framework [4]. To support readers unfamiliar with the ISO terminology, Table 1 provides a mapping between ISO-29100 and GDPR terminology regarding the fundamental concepts associated with personal data processing. Note that this mapping only provides relevant concepts and does not indicate that the concepts are interpreted in the exact same way - for example Sensitive PII in ISO terminology is *similar* to Special Category personal data under GDPR, but they cannot be used interchangeably. Therefore, when applying ISO standards to GDPR, such mappings are indicative of which concepts should be (re-)interpreted with GDPR's definitions and requirements.

Table 1. Mapping between ISO/IEC 29100:2011 and EU GDPR terminology

ISO/IEC 29100:2011	EU GDPR
Section 2.4 Consent	Article 4-11 Consent
Section 2.9 PII	Article 4-1 Personal Data
Section 2.10 PII Controller	Article 4-7 Controller
Section 2.11 PII Principal	Article 4-1 Data Subject
Section 2.12 PII Processor	Article 4-8 Processor
Section 2.23 Processing of PII	Article 4-2 Processing
Section 2.26 Sensitive PII	Article 9 Special Categories of Personal Data
Section 2.27 Third Party	Article 4-10 Third Party

In prior work [14], we analysed and compared ISO-29184 requirements for notice and consent with those in GDPR to understand the extent to which ISO-29184 standard can be applied to demonstrate compliance with the requirements of the GDPR. We also explored the possibility of using ISO-29184 certifications under GDPR for consent and notice. In continuation of that work, Table 2 compares ISO-27560 for consent information and ISO-29184 for privacy notice information with the requirements under GDPR to provide a holistic view of how the two standards can be used to address GDPR's requirements. In this, it is important to note that unlike ISO-29184 which is an international standard, ISO-27560 is what ISO terms a *Technical Specification (TS)* which only provides guidance and is intended to obtain feedback to create a (future) international standard.

Table 2. Mapping information requirements across ISO/IEC TS 27560:2023, ISO/IEC 29184:2020 and EU GDPR. For GDPR, numbers without prefixes are Articles, and with prefix R are Recitals

ISO/IEC TS 27560:2023	ISO/IEC 29184:2020	EU GDPR
3.1 consent	–	4-11 definition of consent
3.2 consent receipt	Annex B	R42, 7-1 demonstrating consent
3.3 consent record	–	R42, 7-1, 13, 14, 30 recording information related to consent
3.4 consent type	5.4.3 Informed and freely given consent. 3.1 explicit consent	R32, R43, 6-1a, 9-2a conditions for consent. R42 demonstrating consent. 8 child’s consent. 9-2a explicit consent
6.2 recordkeeping for privacy notices and consent	–	R42, 7-1, 13, 14, 30 recording and demonstrating consent
6.2.2.1 presentation of notice	5.2.2 providing notice, 5.2.3 appropriate expression, 5.2.7 appropriate forms, 5.2.9 accessibility	R32, R42, R43, R58, 7-2 notice for consent
6.2.2.2 timeliness of notice	5.2.5 appropriate timing	R32, R42, R43, R60, 7-2, 13, 14 notice for providing information and requesting consent. R61, 13-2 14-3 timing of notice. R62 exceptions
6.2.2.3 obtaining consent	5.2.7 appropriate forms	R42, 7-1 record of consent
6.2.2.4 time and manner of consent	5.2.6 appropriate locations	R32, R42, R43, 7-2
6.2.2.5 technical implementation	–	R42, 7-1, 13, 14, 30 maintaining information for demonstrating consent
6.2.2.6 unique reference	5.2.8 ongoing reference	R42, 7-1 demonstrating consent
6.2.2.7 legal compliance	–	R39, 5 principles, 5 principles. R40, R41, 6 lawfulness and legal basis. R50 further processing. R42, 7-1 record of consent
6.3.4.1 privacy_notice	3.2 notice	R32, R42, R43, R60, R61, 7-2, 13, 14 notice for providing information
6.3.4.2 language	5.2.4 multi-lingual notice	R32, R42, R43 conditions for consent
6.3.4.3, 6.3.4.4 purposes	5.3.2 purpose description, 5.3.3 Presentation of purpose description	5, 6-1a, 13-1c, 13-3, 14-1c, 14-4, 15-a, 30-1b purpose of processing
6.3.4.6 lawful_basis	5.3.15 Basis for processing	R40, R41, 6-1a, 7-1a, 9-2a, 13-1c, 13-1d, 14-1c lawfulness and legal basis
6.3.4.7 pii_information	3.3 element of PII	4-1, 14-1d, 15-1b, 30-1c personal data
6.3.4.8 pii_controllers	5.3.4 Identification of the PII controller	13-1a, 14-1a, 30-1a identity of controller
6.3.4.9 collection_method	5.3.5 PII collection, 5.3.6 Collection method, 5.3.7 Timing and location of the PII collection	R61, 13-1, 14-1, 14-2f, 15-1g source of personal data
6.3.4.10 processing_method	5.3.8 Method of use	4-2, 30-2b processing methods. 13-2f, 14-2g, 15-1h automated decision making and profiling
6.3.4.11 storage_locations	5.3.9 Geo-location of, and legal jurisdiction over, stored PII	13-1f, 14-1f, 15-2 storage or processing location
6.3.4.12 retention_period	5.3.11 Retention period	13-2a, 14-2a, 15-1d, 30-1f storage duration or time limits
6.3.4.13 processing_locations	5.3.9 Geo-location of, and legal jurisdiction over, stored PII	13-1f, 14-1f, 15-2 processing location (including data transfers)
6.3.4.14 geo-graphic_restrictions	5.3.9 Geo-location of, and legal jurisdiction over, stored PII	13-1f, 14-1f, 15-2, 30-1e, 30-2c, 44, 45, 46, 47, 48, 49-1a geographic condition (e.g. third country)

continued

Table 2. continued

6.3.4.16 jurisdiction	5.3.9 Geo-location of, and legal jurisdiction over, stored PII	13-1f, 14-1f, 15-2, 30-1e, 30-2c, 44, 45, 46, 47, 48, 49-1a geographic condition (e.g. third country)
6.3.4.17 recipient_third_parties	5.3.10 Third-party transfer	4-9, 4-10, 13-1e, 14-1e, 15-1c, 19, 30-1d recipients
6.3.4.18 withdrawal_method	5.3.12 Participation of PII principal	R42, 7-3, 13-2c, 14-2d withdrawing consent
6.3.4.19 privacy_rights	5.3.12 Participation of PII principal	13-2b, 13-2c, 14-2c, 14-2d, 15-1e, 16, 17, 18, 20, 21, 22 rights of data subject
6.3.4.20 codes_of_conduct	–	24-3, 32-3, 35-8, 40 codes of conduct, 42 certification
6.3.4.21 impact_assessment	5.3.16 Risks	R75, R84 risks and risk evaluation. R90, R91, R92, R93, 35 Data Protection Impact Assessments (DPIA)
6.3.4.22 authority_party	5.3.13 Inquiry and complaint	13-2d, 14-2e, 15-1f complaint to authority. 36-1 consult with authority for impact assessment. 51 supervisory authority, 56 lead authority.
6.3.5.1 pii_type	3.3 element of PII	4-1, 14-1d, 15-1b, 30-1c personal data types and categories
6.3.5.2 pii_attribute_id	3.3 element of PII	–
6.3.5.3 pii_optional	5.4.6 Separate consent to necessary and optional elements of PII	R90, R91, 5, 13-2e, 35 optionality or necessity of personal data
6.3.5.4 sensitive_pii_category	–	R51 protecting sensitive data
6.3.5.5 special_pii_category	–	R51, R53, R71, 6, 9, 22-4, 30-1c, 35 special categories of personal data
6.3.6.6 party_name	–	13-1a, 14-1a, 30-1a, 30-2a
6.3.6.7 party_role	–	4-1, 4-7, 4-7, 4-8, 4-9, 4-10, 13-1a, 13-1e, 14-1a, 14-1e, 26-1, 28, 30-1a, 30-1d, 30-2a, 37
6.3.6.8 party_contact	–	13-1a, 13-1b, 14-1a, 14-1b, 26-1
6.3.6.9 party_type	–	4-1, 4-7, 4-7, 4-8, 4-9, 4-10, 13-1e, 14-1e, 15-1c, 19
6.3.7.1 event_time	5.4.8 Timeliness	R42, 7-1, 13, 14, 30 maintaining information for demonstrating consent
6.3.7.2 validity_duration	5.4.7 Frequency	25 Data Protection by Design and by Default
6.3.7.3 entity_id	–	R42, 4-11, 6-1a, 7-3, 8-1, 8-2, A13, A14
6.3.7.4 event_type	5.4.3 Informed and freely given consent	4-11 (regular) consent. 9-2a explicit consent. R32, 7-1 given consent. R32, 7-2 request for consent
6.3.7.6 event_state	5.5.2 Renewing notice, 5.5 Change of conditions, 5.5.3 Renewing consent	4-11, 6-1a, 9-2a given consent. R42, 7-3 withdrawn consent.
6.4.3 consent management	–	R32, R42, R43, R60, R61, 7-2, 12, 13, 14 information about given consent and applicable rights, R42, 7-3 withdrawing consent
6.4.4 PII principal participation	5.3.12 Participation of PII principal, 5.3.14 Information about accessing the choices made for consent	R32, R42, R43, R60, R61, 7-2, 12, 13, 14 information about given consent and applicable rights, R42, 7-3 withdrawing consent
6.4.6 receipt content	5.3.14 Information about accessing the choices made for consent	R32, R42, R43, R60, R61, 7-2, 12, 13, 14 information about given consent and applicable rights

continued

Table 2. continued

Annex B consent lifecycle	5.5.2 Renewing notice, 5.5 Change of conditions, 5.5.3 Renewing consent	4-11, 6-1a, 9-2a given consent. R42, 7-3 withdrawn consent.
Annex E security of consent records and receipts	–	R75, R76, R77, R78, R83, 24, 25, 30, 32, 44
Annex F signals communicating PII Principal’s preferences and decisions	–	R32, 7-2, 21-5

4 Consent Records and Receipts Using DPV

ISO-27560 only defines the information fields and does not prescribe how they should be technically represented in practice. To implement ISO-27560, the information therefore must be represented in a format such as JSON which is widely supported and easy to use. However, the use of JSON requires a strict agreement on how the information should be structured and how it should be interpreted. The JSON-LD (JSON for Linked Data) format enables use of JSON with linked data so that the ontologies and vocabularies defined using W3C standards can be exchanged as JSON data. For this reason, ISO-27560 Annex C provides examples of consent records and receipts for both JSON and JSON-LD. Implementing ISO-27560 in a machine-readable manner using JSON-LD requires agreement on the schema or ontology to represent the fields. The Annex C JSON-LD example uses the Data Privacy Vocabulary¹ (DPV) [13,15] which is maintained by the W3C Data Privacy Vocabularies and Controls Community Group² (DPVCG).

DPV is a state of the art resource that provides the necessary ontology to represent concepts such as purpose, processing operations, personal data, legal roles, as well as a rich and extensive taxonomy expanding on each of these concepts to enable representing of practical use-cases. For example, using DPV, it is possible to exchange ISO-27560 records and receipts in JSON-LD which specify the *Purpose* is *Marketing* in an interoperable manner. In addition, DPV also features extensions through which different jurisdiction specific concepts can be represented, and for which it provides extensions for EU regulations such as the GDPR, DGA, and the upcoming AI Act. This enables flexibility of expression general requirements such as the *legal basis* should be *consent*, as well as specific requirements such as *explicit consent* as per GDPR Art.9-1a.

DPV was initiated as part of the SPECIAL H2020 project and has been developed for over 6 years with a multi-disciplinary community made up of computer scientists, legal experts, sociologists, data protection officers, industry stakeholders, and authorities. It has been actively used in several projects at national and international (e.g. Horizon Europe) levels, is being used by the industry, and has been acknowledged by within standards (including ISO-27560) [13]. As such, it represents the best resource currently available for representing consent records

¹ <https://w3id.org/dpv>.
² <https://www.w3.org/groups/cg/dpvcg/>.

and receipts as well as other legally relevant information in a machine-readable form that is based on open (free and non-proprietary) interoperable standards.

To support the implementation of use of DPV in implementing consent records and receipts in conformance with ISO-27560 and the GDPR, we have developed a technical specification which can be accessed online at <https://w3id.org/dpv/guides/consent-27560>. The specification describes how the required fields in ISO-27560 and GDPR are represented using DPV (summarised below) and provides illustrative examples for each (see online). Consent records are represented as instances of the concept `dpv:ConsentRecord` and receipts are represented as instances of the concept `dpv:ConsentReceipt`. For reviewers convenience: complete examples of a consent record and a consent receipt are provided in the annexes at the end of this article.

Profiles: To support implementing ISO-27560 as well as its use to comply with GDPR, DPVCG defines 4 schemas or profiles defined under the namespace <https://w3id.org/dpv/schema/dpv-27560#> (prefixed as `dpv-27560:`).

1. [dpv-27560:record](#): Consent Records conforming with ISO-27560.
2. [dpv-27560:record-eu-gdpr](#) Consent Records conforming with ISO-27560 and containing information as required by EU GDPR.
3. [dpv-27560:receipt-record](#) Consent Receipts conforming with ISO-27560 and providing information from consent record(s).
4. [dpv-27560:receipt-eu-gdpr](#) Consent Receipts conforming with ISO-27560 and providing information from consent record(s) as required by EU GDPR.

Metadata Fields: (See Table 3) to describe the generic metadata fields associated with records and receipts, we utilise the DCMI Metadata Terms standard³ (prefixed as `dct:`). A consent record or receipt indicates use of the DPV profiles by using `dct:conformsTo` with one of the profiles described above.

Table 3. DPV concepts for ISO/IEC 27560:2023 Metadata fields

Field	Cardinality	DPV Concept	DPV Property
Schema Version	1	N/A	<code>extttdct:conformsTo</code>
Record Identifier	1..*	N/A	<code>dpv:hasIdentifier</code>
Data Subject	1	<code>dpv:DataSubject</code>	<code>dpv:hasDataSubject</code>

Processing Fields: (See Table 4) ISO-27560 contains 22 fields related to processing activities, and 5 additional fields regarding personal data involved in processing. The structuring of these fields within ISO-27560 is of the form where

³ <https://dublincore.org/specifications/dublin-core/dcmi-terms/>.

the ‘PII Processing’ section contains an array of ‘purposes’ where each ‘purpose’ is expressed with its own fields regarding legal basis, collection method, storage locations, and so on. Within the DPV implementation, this is replaced with `dpv:Process` where each ‘process’ represents a distinct processing activity with its own fields e.g. purposes, personal data, recipients. Thus a consent record and receipt may cover multiple processes (and purposes) which permits an unambiguous and exact representation e.g. which purpose, implemented by which entity, with what data, recipient, etc.

Table 4. DPV concepts for ISO/IEC 27560:2023 Processing fields

Field	Cardinality	DPV Concept	DPV Property
Process	1..*	<code>dpv:Process</code>	<code>dpv:hasProcess</code>
Purpose	1..*	<code>dpv:Purpose</code>	<code>dpv:hasPurpose</code>
Personal Data	1..*	<code>dpv:</code>	<code>dpv:hasPersonalData</code>
Personal Data Type	1..*	<code>dpv:PersonalData</code> taxonomy	<code>dpv:hasPersonalData</code> or <code>dct:type</code>
Personal Data Identifier	0..*	N/A	<code>dct:identifier</code>
Personal Data Necessity	0..*	<code>dpv:Necessity</code>	<code>dpv:hasNecessity</code>
Sensitive/Special Category	0..*	<code>dpv:SensitivePersonalData</code> , <code>dpv:SpecialCategoryPersonalData</code>	<code>dpv:hasPersonalData</code> or <code>dct:type</code>
Processing Operations	0..*	<code>dpv:Processing</code>	<code>dpv:hasProcessing</code>
Data Source	0..*	<code>dpv:DataSource</code>	<code>dpv:hasDataSource</code>
Storage Condition	1..*	<code>dpv:StorageCondition</code> , <code>dpv:StorageLocation</code> , <code>dpv:StorageDuration</code> , <code>dpv:StorageDeletion</code>	<code>dpv:hasStorageCondition</code>
Processing Condition	0..*	<code>dpv:ProcessingCondition</code> , <code>dpv:ProcessingLocation</code> , <code>dpv:ProcessingDuration</code>	<code>dpv:hasProcessingCondition</code>
Geographic Restriction	0..*	<code>dpv:Rule</code>	<code>dpv:hasRule</code>
Data Controller	1..*	<code>dpv:DataController</code>	<code>dpv:hasDataController</code>
Legal Basis	0..*	<code>dpv:LegalBasis</code>	<code>dpv:hasLegalBasis</code>
Recipients	1..*	<code>dpv:Recipient</code>	<code>dpv:hasRecipient</code>
Consent Change & Withdrawal	1..*	<code>dpv:InvolvementControl</code> , <code>dpv:WithdrawingFromActivity</code>	<code>dpv:hasInvolvementControl</code>
Jurisdiction	1..*	<code>dpv:Jurisdiction</code>	<code>dpv:hasJurisdiction</code>
Rights	1..*	<code>dpv:DataSubjectRight</code>	<code>dpv:hasRight</code>
Services	0..*	<code>dpv:Service</code>	<code>dpv:hasService</code>
Code of Conduct	0..*	<code>dpv:CodeOfConduct</code>	<code>dpv:hasOrganisationalMeasure</code>
Impact Assessment	0..*	<code>dpv:ImpactAssessment</code>	<code>dpv:hasAssessment</code>
Notice	1..*	<code>dpv:Notice</code>	<code>dpv:hasNotice</code>
Notice Language	1..*	N/A	<code>dct:language</code>

Entity Fields: (See Table 4) DPV uses the term *Entity* for what ISO-27560 refers to as *Party*. Entities are expressed using instances of `dpv:Entity` and associated using `dpv:hasEntity`. DPV also distinguishes between *Entities* and *Legal Entities* - and their representatives or agents, through which it can be accurately represented whether a party in a consent record acted on their own or it was someone acting on their behalf. This is of relevance for implementations such as consent for children which involves parents or guardians, or even data intermediaries under DGA which can act to support individuals in consent decision making.

Table 5. DPV concepts for ISO/IEC 27560:2023 Party fields

Field	Cardinality	DPV Concept	DPV Property
Name	1..*	N/A	dvp:hasName
Identifier	1..*	N/A	dvp:hasIdentifier
Role	1..*	dvp:DataController, dvp:DataProcessor, dvp:ThirdParty, dvp:Authority, dvp:DataSubject	dvp:hasEntity, dvp:hasDataController, dvp:hasDataProcessor, dvp:hasThirdParty, dvp:hasAuthority, dvp:hasDataSubject
Contact	1..*	schema:ContactPoint	schema:contactPoint
Postal Address	1..*	schema:PostalAddress	schema:contactPoint
Email	0..*	N/A	schema:email
Phone	0..*	N/A	schema:telephone
URL	0..*	N/A	schema:url

Consent Event Fields: (See Table 5) These fields are used to indicate the type of consent (e.g. *Implicit*, *Expressed*, *Explicit*) as expressed by the data subject. In DPV, **dvp:ConsentType** represents consent types to be used as a legal basis and has the following different types: *Informed* with specialisations for *Implied* when implied or given by an indirect action (e.g. merely browsing a website), *Expressed* for direct expressed action (e.g. a checkbox), and *ExplicitlyExpressed* for direct action concerning solely the consent in context. To indicate consent types as defined in GDPR, the DPV's GDPR extension is used e.g. **eu-gdpr:A6-1-a** for expressed consent and **eu-gdpr:A9-2-a** for explicit consent.

In addition to the type of consent, these fields also enable expressing the status of consent, such as whether it has been requested, given, refused, expired, terminated, invalidated, or re-affirmed. Each event can contain metadata to indicate when it took place (e.g. date when consent was given), how it was expressed (e.g. in the account dashboard), its duration (e.g. validity of given consent), and by whom (e.g. the data subject).

Table 6. DPV concepts for ISO/IEC 27560:2023 Event fields

Field	Cardinality	DPV Concept	DPV Property
Consent Type	1..*	dvp:Consent taxonomy	dvp:hasLegalBasis
Consent State	1..*	dvp:ConsentStatus taxon- omy	dvp:hasConsentStatus
Event Time	1..*	N/A	dvp:isIndicatedAtTime
Event Duration	1..*	dvp:Duration	dvp:hasDuration
Expression by Entity	1..*	dvp:Entity	dvp:isIndicatedBy
Expression Method	0..*	N/A	dvp:hasIndicationMethod

Consent Receipts: (See Table 7) ISO-27560 only defines the schema version and receipt identifier fields for consent receipts. For other fields, it recommends using the same fields as that of a consent record. In its guidance, it states that the mandatory fields in consent records should also be mandatory in receipts. Based on this, we only define the additional fields for consent receipts and suggest reusing the consent record fields with their necessity/optionality requirements. Therefore, a consent receipt only has three mandatory fields with the rest of the information being present as instances of consent record(s).

Table 7. DPV concepts for ISO/IEC 27560:2023 Receipt Metadata fields

Field	Cardinality	DPV Concept	DPV Property
Schema Version	1	N/A	dct:conformsTo
Receipt Identifier	1..*	N/A	dpv:hasIdentifier
Consent Record	1..*	dpv:ConsentRecord	dpv:hasRecordOfActivity

5 Supporting GDPR and DGA

Using ISO-27560 and ISO-29184 Within the EU Legal Framework: ISO-27560 and ISO-29184 are developed and governed by the International Standards Organisation (ISO), and are not specific to EU’s regulations and terminology. To support their use in the legal frameworks, they need to be approved as ‘Euronorm’ (EN) through an EU standardisation body such as CEN, CEN-ELEC, or ESO. At the moment, ISO-29184 has already been approved as EN, and we are working on a proposal with the Irish and Swedish national bodies to recommend the adoption of ISO-27560 as EN. Further, we have also submitted a proposal to the relevant ISO committees to make ISO-27560 standard freely accessible as its guidance is valuable for responsible innovation.

Having these standards as EN provides a strong framework for their utilisation in regulations, such as for notice and consent under GDPR. However, merely adopting the standards on an ‘as-is’ basis will not be sufficient. For example, the terminology in 29184 and GDPR has crucial differences which must be identified and appropriate guidance developed to enable using ISO-29184 with GDPR [14]. Similarly, to address current issues regarding consent [10, 11] and further studies are required to assess the extent of these standards in solving existing issues and what additional measures need to be adopted beyond conformance with the standards.

Demonstrating Consent Under GDPR: GDPR Article 7-1 creates an obligation for data controllers to maintain consent information and to keep it up to date with the goal of demonstrating where consent was given, refused, or

withdrawn. ISO-27560 provides a standard for a common technical structure to support implementing this obligation. In addition to this, GDPR Article 13 and Article 14, amongst others, also require record keeping for what information was provided to individuals in order to implement informed consent. ISO-29184 provides a standard for describing privacy notices, and together with ISO-27560 enables maintaining records of what information was provided and the resulting consent decisions. Based on the analysis provided in this article that demonstrates applicability of ISO-27560 and ISO-29184 to GDPR, we recommend authorities to suggest using these standards to support GDPR compliance.

Receipts to Support Rights Under GDPR: ISO-27560 contains fields for acknowledging which rights exist, and with DPV we can express how/where to exercise them and what information will be required (e.g. identity verification). Further, consent decisions (e.g. given, withdrawn) are themselves also personal data about the data subject, and therefore subject to rights such as Article 20 data portability. This can be a way to enable the use of receipts under GDPR even where it is not explicitly defined as a concept by considering consent information as *personal data*. Considering consent information as personal data makes it subject to the right to data portability under Article 20 which requires providing information “in a structured, commonly used and machine-readable format”. Further, Article 20 also allows “the right to transmit those data to another controller”, which can be utilised to transfer consent decisions from one controller to another - a crucial mechanism for the implementation of data reuse and altruism under DGA.

Common Consent Form Under DGA: Article 25 of the DGA requires the Commission to produce a common consent form that will provide information in both human- and machine-readable forms. ISO-27560 with ISO-29184, based on the analysis in this article demonstrating their usefulness to meet GDPR requirements, should be used to define what information should be present in these forms. ISO-29184 as the standard for privacy notices provides the human-oriented representation of information in the consent form, and ISO-27560 and the DPV implementation provide the machine-readable representation. The advantage of using these standards is that the resulting solution would be useful not only in EU but globally due to the global scope of ISO. The advantage of using DPV here is in providing common semantics based on W3C standards that support extensions for specific jurisdictions (like EU with GDPR and DGA) and its extensive taxonomy supporting practical use-cases which promote interoperability. **Through direct meetings, we have presented this work to the EU Commission’s Unit G.1 which looks after GDPR and DGA implementations.**

Data Intermediaries Under DGA: We are also working on further implementations to support DGA by developing specific technical specifications

that define how data intermediaries should maintain consent records and issue receipts, and support them in their duties by providing a way to express data reuse requests in a machine-readable form that can be matched with the consent to ensure the purposes are compatible in accordance with the GDPR. This will be based on existing work [1] that utilises the W3C Open Digital Rights Language (ODRL) standard [3] for representing policies and agreements, and using it in combination with DPV to create DGA specific *offers* for data subjects and data intermediaries to indicate which data is available for reuse and under what conditions, requests for data users to indicate what data they are looking for, and *agreements* to represent the conditions under which data reuse has been approved. We have already demonstrated the feasibility of using ODRL and DPV for such an approach in a manner that improves both technical and organisational processes for the use-case of sharing genomic health datasets [12].

Data Reuse and Altruism Under DGA: To support the DGA’s goals of reusing data for altruism, we are working on creating a taxonomy of altruistic purposes within DPV and developing a framework to express them in a manner that is compatible with GDPR’s requirements for consent and information keeping based on ISO-27560. We are also working on novel approaches such as assessing the compatibility of ISO-27560 defined consent records with information required in a Data Protection Impact Assessment (DPIA), through which we aim to enable data subjects or data intermediaries to conduct their own DPIAs based on a common registry of risks and mitigations provided through the DPV. Through this we aim to establish responsible practices while promoting data reuse and altruism.

6 Implementation Considerations and Future Work

6.1 Trust and Security

Security considerations are extremely important in the implementation of consent records and receipts, with ISO-27560 Annex E providing guidance for implementations. Consent records are intended to be maintained internally by an entity, and require measures to ensure they maintain their consistency and correctness, and are not tampered with. This includes best practices for information management such as using cryptographic hashes to ensure information has not changed, or using access control to ensure only authorised modifications are permitted. Current international standards such as W3C Decentralized Identifiers⁴ (DID) and W3C Verifiable Credentials⁵ (VC) allow for implementations compatible with the implementation of ISO-27560 using DPV as all are based on interoperable semantic web standards.

For consent receipts to be utilised in a verifiable and trustworthy manner, the information provided within the receipt may require cryptographic measures

⁴ <https://www.w3.org/TR/vc-data-model/>.

⁵ <https://www.w3.org/TR/did-core/>.

to provide assurance to prove its immutability and non-repudiation. Further, receipts are intended to be information provided or exchanged between different entities, which may necessitate a mechanism to demonstrably verify the provenance (e.g. a receipt was provided by A to B) and its immutability (e.g. receipt contained X exactly). Cryptography techniques such as digital signatures and certificates can support such applications based on their current utilisation in internet-enabled applications and documentations. Prior work [7] and projects⁶ have explored such considerations, but effective implementation requires consensus amongst stakeholders to create an interoperable ecosystem.

Given the role of consent records and receipts in demonstrating consent decisions, they may end up with potentially sensitive information. ISO-27560 recommends not putting such information directly in records and receipts, and if necessary then implementations should utilise techniques such as information masking or pseudonymisation to avoid directly exposing sensitive information. - though this has to be balanced with the purpose of receipts in providing data subjects with information about their consent.

6.2 Using Records and Receipts with eIDAS and EUDI Wallet

Following the launch of projects for using European Digital Identity wallet (EUDI) wallet⁷ for travel, health, banking, education and other sectors, CEN TC224 WG20⁸, which is the EU standardisation body's technical committee for personal identification, has initiated a new standards project to provide guidance on when personal data (attributes) are shared from the wallet in compliance with eIDAS and its proposed revision.

In this, ISO-27560 and ISO-29184 can be used to create an interoperable and standards based mechanism to structure information and ensure the mandatory fields needed to comply with GDPR are present. Further, the use of these standards also enables a consistent approach for creating common privacy dashboards that can work across EU. Such privacy dashboards would allow a wallet holder to have an overview of all their consent transactions, including any pending requests as well as provide a centralised mechanism for controlling their rights and withdrawing consent by using the eIDAS and eID mechanisms to establish identity and proof of past engagement.

ISO-27560 and ISO-29184 are also crucial as being the only standards regarding consent records and receipts, and privacy notices respectively. Using the analysis and implementations described in this article, a ISO-27560 solution that is also conformant with the GDPR can be used to store consent records and receipts in wallets, which enables data subjects to have a copy of their decision and agreement to process personal data.

⁶ NGI funded Privacy as Expected: Consent Gateway project D2 Final Technical Deliverable <https://doi.org/10.5281/zenodo.5086238>.

⁷ <https://digital-strategy.ec.europa.eu/en/news/eu-digital-identity-4-projects-launched-test-eudi-wallet>.

⁸ <https://www.cencenelec.eu/areas-of-work/cen-sectors/digital-society-cen/information-and-identification-systems/>.

Having this information made available to the data subject in a machine-readable format further enables its use in innovative applications that promote reuse of data while ensuring adequate adherence to the EU's values and regulations. For example, by looking at past consent records or receipts, preferences can be identified for how the individual makes decisions and these can be used to create a template or pattern that will make future consent decisions more efficient and simpler for the individual. ISO-27560 Annex F provides guidance on how such preferences used as 'privacy signals' can be represented within consent records and receipts.

Another powerful paradigm is also made possible when combining ISO-27560 with eID, eIDAS, and EUDI - where the data subject initiates the consent process by providing a specific consent to use or reuse their personal data, for example to access a particular service. In this scenario, the data subject decides the extent and limit of what their consent will cover, provides their consent to the service provider, and maintains a consent record within their wallet with a signed receipt provided to the service provider as proof of consent.

6.3 Standard for PII Processing Record Information

Even though ISO-27560 only focuses on consent records and receipts, its fields were developed with the intention of a future expansion in a separate standard to cover other legal bases, such as the 7 other legal basis in GDPR Article 6. To continue in this direction, we have initiated a 'new standard' proposal in ISO regarding 'PII processing record information'.

To support this activity, we are currently identifying the specific requirements for record keeping for each legal basis and creating the necessary specifications using DPV. This builds on prior work providing a machine-readable Records of Processing Activities (ROPA) required under GDPR Article 30, and which consolidates the guidelines from all 30 EU/EEA member states.

6.4 Technical Considerations in Managing Records and Receipts

We can use the Data Catalog Vocabulary⁹ (DCAT), a W3C standard, to represent the records as datasets and receipts as a catalogue of records. By doing so, the metadata fields provided by DCAT can be readily used to represent information that supports in maintenance and exchange of consent records and receipts, including using existing infrastructure to manage them. DCAT is a widely used standard that supports implementing (open) data portals and has tooling for discovery and management of information. The EU has developed the DCAT Application Profile¹⁰ (DCAT-AP) which extends DCAT to support the EU Open Data Portals¹¹.

⁹ DCAT - Version 3 <https://www.w3.org/TR/vocab-dcat-3/>.

¹⁰ DCAT Application profile for data portals in Europe (DCAT-AP) <https://op.europa.eu/en/web/eu-vocabularies/dcat-ap>.

¹¹ <https://data.europa.eu/>.

Through these records and receipts can be readily communicated as interoperable datasets between relevant entities - for example controller to data subject, or between controllers and third parties. This is a crucial technical enabler for the principle of increasing data value through utilisation within the Data Governance Act and Data Spaces. In particular, the use of DCAT(-AP) also supports the addition of further policies and measures to support the implementation of data intermediaries which will be required to maintain consent records under the obligations of the DGA.

6.5 IEEE P7012 Machine-Readable Privacy Terms

In addition to the above, we are also working with the IEEE P7012 group to develop a standard for machine-readable privacy terms which uses ISO-27560 and ISO-29184 with DPV to define the conditions under which the individual allows use or reuse of their personal data. The use of this standard will provide an efficient and optimal mechanism for data subjects to signal their consent or initiate an agreement with a service provider.

7 Conclusion

This article provided a thorough analysis of how ISO/IEC TS 27560:2023 and ISO/IEC 29184:2020 can be used to create consent records and receipts in a machine-readable format that support GDPR requirements and enable the reuse of data under the DGA. Based on this analysis, we provide a concrete argument for why these two standards should be adopted and recommended by GDPR stakeholders. We also described the ongoing efforts of the W3C Data Privacy Vocabularies and Controls Community Group (DPVCG) in creating a technical specification to support implementing ISO-27560 by using its Data Privacy Vocabulary (DPV). Our work is a significant contribution to the ongoing efforts of implementing the DGA where the Commission is required to develop a common consent form that is both human- and machine-readable. We also discussed how this work can be utilised in practice, where reported on our ongoing efforts to adopt the standard within the EU's legal framework, further develop specific implementations to support the needs of DGA, and how this work compliments the ongoing developments of eID, eIDAS2, and EUDI implementations.

Acknowledgements. Jan Lindquist, through the Swedish National Standards Body, was a contributor and the co-editor of ISO/IEC TS 27560:2023. Harshvardhan J. Pandit, through the Irish National Standards Body, was a contributor to the ISO/IEC TS 27560:2023, and is the chair of the W3C Data Privacy Vocabularies and Controls Community Group.

This research was conducted with the financial support of Science Foundation Ireland at ADAPT, the SFI Research Centre for AI-Driven Digital Content Technology at Dublin City University Grant#13/RC/2106.P2. For the purpose of Open Access, the author has applied a CC BY public copyright licence to any Author Accepted Manuscript version arising from this submission.

A Example of Consent Record with both Required and Optional Fields

```

1  {
2    "@id": "https://example.com/a6f58318-72e6-46a2-bfd7-f36d795e30cd",
3    "@type": "dpv:ConsentRecord",
4    "dct:identifier": "a6f58318-72e6-46a2-bfd7-f36d795e30cd",
5    "dct:conformsTo": "https://w3id.org/dpv/schema/dpv-27560#record",
6    "dpv:hasDataSubject": {
7      "@id": "0760c9ba",
8      "type": "dpv:Consumer"
9    },
10   "dpv:hasDataController": "ex:Acme",
11   "dpv:hasDataProcessor": "ex:Beta",
12   "dpv:hasJurisdiction": ["loc:IE"],
13   "dpv:hasApplicableLaw": "eu-gdpr:GDPR",
14   "dpv:hasLegalBasis": "eu-gdpr:A6-1-a",
15   "dpv:hasProcess": {
16     "@type": "dpv:Process",
17     "dpv:hasService": "Register for Event X",
18     "dpv:hasRecipient": ["ex:Acme", "ex:Beta"],
19     "dpv:hasPurpose": "dpv:PaymentManagement",
20     "dpv:hasPersonalData": {
21       "@type": "pd:EmailAddress",
22       "rdf:value": "hello@example.com",
23       "dpv:hasNecessity": "dpv:Optional",
24       "dpv:hasDataSource": "dpv:DataSubject",
25     },
26     "dpv:hasStorageCondition": [{
27       "@type": "dpv:StorageLocation",
28       "dpv:hasLocation": ["loc:IE", "loc:FR", "loc:DE"],
29     }, {
30       "@type": "dpv:StorageDuration",
31       "dpv:hasDuration": "P6M",
32     }, {
33       "@type": "dpv:StorageDeletion",
34       "dpv:hasDuration": "P1M"
35     }]
36   },
37   "dpv:hasProcess": {
38     "@type": "dpv:Process",
39     "dpv:hasService": "Register for Event X",
40     "dpv:hasRecipient": ["ex:Acme", "dpv:DataSubject"],
41     "dpv:hasPurpose": "dpv:IdentityVerification",
42     "dpv:hasPersonalData": {
43       "@type": "pd:OfficialID",
44       "dct:identifier": "XJ189019D",
45       "dpv:hasNecessity": "dpv:Required",
46       "dpv:hasDataSource": "ex:Acme",
47     },
48     "dpv:hasStorageCondition": [{
49       "@type": "dpv:StorageLocation",
50       "dpv:hasLocation": "dpv:WithinDevice",

```

```
51     }, {
52       "@type": "dpv:StorageDuration",
53       "dpv:hasDuration": {
54         "@type": "dpv:UntilEventDuration",
55         "rdf:value": "Account Closure"
56       }
57     },
58     "dpv:hasNotice": {
59       "@id":
60         ↪ "https://example.com/notices/a6f58318-72e6-46a2-bfd7-f36d795e30cd",
61       "@type": "dpv:ConsentNotice",
62       "dct:date": "2024-01-01",
63       "dct:language": "EN",
64       "dct:coverage": "2024-01-01/P12M"
65     }
66     "dpv:hasImpactAssessment": {
67       "@type": "dpv:DPIA",
68       "schema:url": "https://example.com/DPIA"
69     }
70     "dpv:hasInvolvementControl": {
71       "@type": ["dpv:ProvidingPermission", "dpv:WithdrawingPermission"],
72       "dpv:isExercisedAt": "https://example.com/manage-consent"
73     },
74     "dpv:hasRight": [{
75       "@type": ["dpv:DataSubjectRight", "eu-gdpr:A7-3"],
76       "dct:title": "Right to Withdraw Consent",
77       "dpv:isExercisedAt": "https://example.com/rights",
78     }],
79     "dpv:hasConsentStatus": [{
80       "@type": ["dpv:ConsentGiven", "dpv:ExpressedConsent"],
81       "dpv:isIndicatedBy": "dpv:DataSubject",
82       "dpv:hasIndicationMethod": "Interaction in App",
83       "dpv:isIndicatedAtTime": "2024-01-01"
84     }], {
85       "@type": "dpv:ConsentWithdrawn",
86       "dpv:isIndicatedBy": "dpv:DataSubject",
87       "dpv:hasIndicationMethod": "Interaction in App",
88       "dpv:isIndicatedAtTime": "2024-04-20"
89     }
90   ]
91 }
```

B Example of Consent Receipt with Required Fields from Consent Record

```
1 {
2   "@id": "https://example.com/receipt-asdmjload",
3   "@type": "dpv:ConsentRereceipt",
4   "dct:identifier": "receipt-asdmjload",
5   "dct:conformsTo": "https://w3id.org/dpv/schema/dpv-27560#receipt",
6   "dct:created": "2024-01-31",
```

```

7      "dct:publisher": "ex:Acme",
8      "schema:recipient": "dpv:DataSubject",
9      "dpv:hasRecordOfActivity": {
10         "@id": "https://example.com/a6f58318-72e6-46a2-bfd7-f36d795e30cd",
11         "@type": "dpv:ConsentRecord",
12         "dct:identifier": "a6f58318-72e6-46a2-bfd7-f36d795e30cd",
13         "dct:conformsTo": "https://w3id.org/dpv/schema/dpv-27560#record",
14         "dpv:hasDataSubject": {
15             "@id": "0760c9ba",
16             "type": "dpv:Consumer"
17         },
18         "dpv:hasDataController": "ex:Acme",
19         "dpv:hasDataProcessor": "ex:Beta",
20         "dpv:hasJurisdiction": ["loc:IE"],
21         "dpv:hasApplicableLaw": "eu-gdpr:GDPR",
22         "dpv:hasProcess": {
23             "@type": "dpv:Process",
24             "dpv:hasRecipient": ["ex:Acme", "ex:Beta"],
25             "dpv:hasPurpose": "dpv:PaymentManagement",
26             "dpv:hasPersonalData": "pd:EmailAddress",
27             "dpv:hasStorageCondition": [{
28                 "@type": "dpv:StorageLocation",
29                 "dpv:hasLocation": ["loc:IE", "loc:FR", "loc:DE"]
30             }, {
31                 "@type": "dpv:StorageDuration",
32                 "dpv:hasDuration": "P6M"
33             }, {
34                 "@type": "dpv:StorageDeletion",
35                 "dpv:hasDuration": "P1M"
36             }]
37         },
38         "dpv:hasProcess": {
39             "@type": "dpv:Process",
40             "dpv:hasRecipient": ["ex:Acme", "dpv:DataSubject"],
41             "dpv:hasPurpose": "dpv:IdentityVerification",
42             "dpv:hasPersonalData": "pd:OfficialID",
43             "dpv:hasStorageCondition": [{
44                 "@type": "dpv:StorageLocation",
45                 "dpv:hasLocation": "dpv:WithinDevice"
46             }, {
47                 "@type": "dpv:StorageDuration",
48                 "dpv:hasDuration": {
49                     "@type": "dpv:UntilEventDuration",
50                     "rdf:value": "Account Closure"
51                 }
52             }]
53         },
54         "dpv:hasInvolvementControl": {
55             "@type": ["dpv:ProvidingPermission", "dpv:WithdrawingPermission"],
56             "dpv:isExercisedAt": "https://example.com/manage-consent"
57         },
58         "dpv:hasRight": {
59             "@type": ["dpv:DataSubjectRight", "eu-gdpr:A7-3"],
60             "dct:title": "Right to Withdraw Consent",

```

```

61         "dpv:isExercisedAt": "https://example.com/rights"
62     },
63     "dpv:hasNotice": {
64         "@id":
65         ↪ "https://example.com/notices/a6f58318-72e6-46a2-bfd7-f36d795e30cd",
66         "@type": "dpv:ConsentNotice",
67         "dct:date": "2024-01-01",
68         "dct:language": "EN",
69         "dct:coverage": "2024-01-01/P12M"
70     },
71     "dpv:hasConsentStatus": [{
72         "@type": ["dpv:ConsentGiven", "dpv:ExpressedConsent"],
73         "dpv:isIndicatedBy": "dpv:DataSubject",
74         "dpv:hasIndicationMethod": "Interaction in App",
75         "dpv:isIndicatedAtTime": "2024-01-01"
76     }, {
77         "@type": "dpv:ConsentWithdrawn",
78         "dpv:isIndicatedBy": "dpv:DataSubject",
79         "dpv:hasIndicationMethod": "Interaction in App",
80         "dpv:isIndicatedAtTime": "2024-04-20"
81     }]
82 }

```

References

1. Esteves, B., Pandit, H.J., Rodríguez-Doncel, V.: ODRL profile for expressing consent through granular access control policies in solid. In: 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), pp. 298–306 (2021). <https://doi.org/10.1109/EuroSPW54576.2021.00038>
2. Esteves, B., Rodríguez-Doncel, V.: Analysis of ontologies and policy languages to represent information flows in GDPR. *Semantic Web* (Preprint) 1–35 (2022)
3. Iannella, R., Villata, S.: ODRL Information Model 2.2 (2018). <https://www.w3.org/TR/odrl-model/>
4. ISO/IEC 29100:2011 Information technology—Security techniques—Privacy framework. Technical report, International Standards Organisation (ISO) (2011)
5. ISO/IEC: ISO/IEC 29184:2020 Information technology – Online privacy notices and consent (2020)
6. ISO/IEC: ISO/IEC TS 27560:2023 Privacy technologies—Consent record information structure (2021)
7. Jesus, V., Pandit, H.J.: Consent receipts for a usable and auditable web of personal data. *IEEE Access* **10**, 28545–28563 (2022). <https://doi.org/10.1109/ACCESS.2022.3157850>
8. Kurteva, A., Chhetri, T.R., Pandit, H.J., Fensel, A.: Consent through the lens of semantics: state of the art survey and best practices. *Semantic Web* 1–27 (2021)
9. Lizar, M., Turner, D.: Consent Receipt Specification v1.1.0. Technical report, Kantara Initiative (2017)
10. Machuletz, D., Böhme, R.: Multiple purposes, multiple problems: a user study of consent dialogs after GDPR. *Proc. Priv. Enhanc. Technol.* **2020**(2), 481–498 (2020)

11. Matte, C., Santos, C., Bielova, N.: Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers? In: Annual Privacy Forum (APF 2020) (2020)
12. Pandit, H.J., Esteves, B.: Enhancing Data Use Ontology (DUO) for health-data sharing by extending it with ODRL and DPV. *Semantic Web* 1–26 (2024). <https://doi.org/10.3233/SW-243583>
13. Pandit, H.J., Esteves, B., Krog, G.P., Ryan, P., Golpayegani, D., Flake, J.: Data privacy vocabulary (dpv)–version 2. In: OSF (2024). [arXiv:2404.13426](https://arxiv.org/abs/2404.13426). <https://doi.org/10.31219/osf.io/ma9ue>
14. Pandit, H.J., Krog, G.P.: Comparison of notice requirements for consent between ISO/IEC 29184: 2020 and general data protection regulation. *J. Data Protect. Priv.* **4**(2), 193–204 (2021)
15. Pandit, H.J., et al.: Creating a vocabulary for data privacy. In: The 18th International Conference on Ontologies, DataBases, and Applications of Semantics (ODBASE2019), Rhodes, Greece, p. 17 (2019)
16. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* **L119** (2016)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

